VERITAS NetBackup Advanced Reporter 4.5™

System Administrator's Guide

for UNIX and Windows

March 2002
30-000516-011

VERITAS

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Copyright

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
Phone 650–527–8000
Fax 650–527–2908
www.veritas.com

Contents

Alphabetical List of Reports

Preface

NetBackup Advanced Reporter 4.5 (NBAR) is a storage management monitoring tool designed to simplify the task of monitoring and reporting on an organization's VERITAS NetBackup activities. If you have a GDM domain set up, you can use NBAR to monitor multiple NetBackup master servers. This version of NBAR supports Windows, Solaris, and HP-UX platforms.

Organization

The *VERITAS NetBackup Advanced Reporter 4.5 System Administrator's Guide* describes how to install the NBAR program, how to operate the user interface, and how to generate and interpret the various reports.

This book consists of this preface followed by the chapters and appendices described below:

Chapter 1, "NBAR 4.5 Architecture," provides an overview of NBAR architecture, for stand-alone NBAR installations and for NBAR with GDM installations.

Chapter 2, "Installing NetBackup Advanced Reporter," provides details on both UNIX and Windows installations, including requirements, supported platforms, and installation procedures.

Chapter 3, "Introduction to the NBAR Reports," explains how to navigate the NBAR interface and tailor the reports to get the information you want.

Chapter 4, "Viewing the Management Reports," provides information on full, incremental, and catalog backups, restore jobs, and error log summaries.

Chapter 5, "Viewing the Administrative Reports," provides job and site summaries, error reports, and details on backup and restore jobs.

Chapter 6, "Viewing the Media Reports," provides details on media use.

Chapter 7, "Viewing the Performance Reports," provides details on system performance.

Chapter 8, “Viewing the End User and Misc. Reports,” provides details on the job history report, and all reports only available through drill-down from another report. These include the error code reports, the *NetBackup Trouble Shooting Guide,* and the job details report.

Chapter 9, “Viewing the GDM Reports,” provides details on the reports which summarize the state of servers in a GDM environment.

Chapter 10, “Administrative Tasks,” provides information on the configuration utility and explains the upgrade process for NBAR.

Chapter 11, “Troubleshooting NBAR,” provides information on known issues.

Appendix A, “Database Schema for NBAR,” provides details on NBAR’s database schema.

Related Documents

The *NetBackup Advanced Reporter System Administrator’s Guide* contains details specific to the VERITAS NetBackup Advanced Reporter 4.5 application. The Guide is available in HTML format and as a PDF file. You can access the HTML version through the **HelpTopics** menu item on the **Help** menu. The PDF version resides with the other PDF documents in the \Doc directory.

Other documents you can refer to include:

- the *NetBackup System Administrator’s Guide,*
- the *NetBackup Trouble Shooting Guide,*
- the *NetBackup User’s Guide,*
- Your web browser’s user documentation.

Online Documentation

On Windows

The released software contains on-line PDF and ASCII versions of the release notes and a readme file for the client. If you choose to install the documentation during setup, NetBackup installs it to the following locations on your disk:

- *install_path*\Help\

  Adobe Acrobat Portable Document Format (PDF) copies of all related documents, including the release notes.

- The readme files on *install_path*\NetBackup\ are:
  - Readme.txt (The Readme.txt file (ASCII format) may be slightly more up-to-date than the printed and pdf copies of the release notes.)
  - Readme_Client.txt
  - Readme_Server.txt
  - Readme_SMS.txt
  - Readme_Win2000.txt

On UNIX

During NetBackup installation, a text copy of the *NetBackup Media Manager Device Configuration Guide* is installed in

/usr/openv/volmgr/MediaMgr_DeviceConfig_Guide.txt

You can copy example code from the device configuration guide if you need to reconfigure the kernel to provide specific tape or optical peripheral support.

The product CD-ROM also contains PDF copies of these release notes and other documents.

Note You will need Adobe Acrobat Reader to view the PDF documents. The latest version of Acrobat Reader is available on the Adobe web site: http://www.adobe.com.
VERITAS assumes no responsibility for the correct installation or use of the reader.

On the Support Web Site

Copies of NetBackup documentation are also available on the VERITAS support web site:

1. Go to the VERITAS support web page

   www.support.veritas.com/

2. In the **VERITAS Support Product List**, choose **NetBackup Products**.

3. A page appears with a list of the NetBackup products. Choose **NetBackup BusinesServer** or **NetBackup DataCenter**.

4. The documents page appears. Choose the document you want.

Conventions

The following explains typographical and other conventions used in this guide.

Type Style

Typographic Conventions

Typeface	Usage
`Bold fixed width`	Input. For example, type **`cd`** to change directories.
`Fixed width`	Paths, commands, filenames, or output. For example: The default installation directory is `/opt/VRTSxx`.
Italics	Book titles, new terms, or used for emphasis. For example: *Do not* ignore cautions.
Sans serif (italics)	Placeholder text or variables. For example: Replace *filename* with the name of your file.
Serif (no italics)	Graphical user interface (GUI) objects, such as fields, menu choices, etc. For example: Enter your password in the **Password** field.

Notes and Cautions

Note This is a Note. Notes are used to call attention to information that makes using the product easier or helps in avoiding problems.

Caution This is a Caution. Cautions are used to warn about situations that could cause data loss.

Key Combinations

Some keyboard command sequences use two or more keys at the same time. For example, holding down the **Ctrl** key while pressing another key. Keyboard command sequences are indicated by connecting the keys with a plus sign. For example:

Press Ctrl+t

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

command *arg1* | *arg2*

the user can use either the *arg1* or *arg2* variable.

Terms

The terms listed in the table below are used in the VERITAS NetBackup documentation to increase readability while maintaining technical accuracy.

Term	Definition
Microsoft Windows, Windows	Terms used as nouns to describe a line of operating systems developed by Microsoft, Inc. A term used as an adjective to describe a specific product or noun. Some examples are: Windows 95, Windows 98, Windows NT, Windows 2000, Windows servers, Windows clients, Windows platforms, Windows hosts, and Windows GUI. Where a specific Windows product is identified, then only that particular product is valid with regards to the instance in which it is being used. For more information on the Windows operating systems that NetBackup supports, refer to the VERITAS support web site at `http://www.support.veritas.com`.
Windows servers	A term that defines the Windows server platforms that NetBackup supports; those platforms are: Windows NT and Windows 2000.
Windows clients	A term that defines the Windows client platforms that NetBackup supports; those platforms are: Windows 95, 98, ME, NT, 2000, XP (for 32- and 64-bit versions), and LE.

Getting Help

For updated information about this product, including system requirements, supported platforms, supported peripherals, and a list of current patches available from Technical Support, visit our web site:

`http://www.support.veritas.com/`

VERITAS Customer Support has an extensive technical support structure that enables you to contact technical support teams that are trained to answer questions to specific products. You can contact Customer Support by sending an e-mail to support@veritas.com, or by finding a product-specific phone number from the VERITAS support web site. The following steps describe how to locate the proper phone number.

1. Open `http://www.support.veritas.com/` in your web browser.
2. Click **Contact Support**. The *Contacting Support Product List* page appears.
3. Select a product line and then a product from the lists that appear. The page will refresh with a list of technical support phone numbers that are specific to the product you just selected.

Accessibility

NetBackup contains features that make the user interface easier to use by people who are vision impaired and by people who have limited dexterity. Accessibility features include:

- Support for assistive technologies such as screen readers and voice input (Windows servers only)
- Support for keyboard (mouse-less) navigation using accelerator keys and mnemonic keys

For more information about accessibility in NetBackup, see the NetBackup system administrator's guide.

NBAR 4.5 Architecture 1

This chapter describes the structure of VERITAS NetBackup Advanced Reporter 4.5.

Note The first part of this chapter applies to all NBAR configurations. The second section applies only if you are planning to run NBAR in a Global Data Management (GDM) environment.

Introduction

VERITAS NetBackup Advanced Reporter 4.5 (NBAR) is a storage management monitoring tool designed to simplify the task of monitoring and reporting on an organization's NetBackup activities.

Why Use NBAR?

NBAR provides a sophisticated reporting option to NetBackup customers. Rather than wading through the text files that make up NetBackup logs, NBAR presents the data you want to see in a succinct and intuitive format, on web pages available from any browser. The available reports help you analyze your NetBackup environment by presenting NetBackup data from four broad viewpoints:

- High level summaries, which allow you to drill down to the specific trouble spots
- Detailed operational views, including a consolidated error log
- Historical perspective for trend analysis and event / time correlation
- Performance indicators, such as data throughput

Many of these reports can be tailored to provide exactly the information you need. NBAR also includes an on-line version of the *NetBackup Trouble Shooting Guide*. Descriptions of all VERITAS NetBackup error codes and the recommended action are only a mouse click away.

NBAR collects and reports on data generated by a NetBackup master server. The portrait of your NetBackup system provided by NBAR gives you an easily accessible overview of the health of your backup environment. NBAR with GDM collects and reports on data generated by multiple NetBackup master servers, providing a global perspective on your network.

How NBAR Works

NBAR takes advantage of NetBackup's client / server architecture. The application is installed on a NetBackup master server, and creates an open-schema database there. NBAR passively scans the VERITAS NetBackup logs for specific information about each client, and copies that information to its own database, then uses that data to generate reports on NetBackup backup and restore activities, catalog operations, and media usage.

NBAR consolidates VERITAS NetBackup information into reports that are easy to read and understand. These reports allow you to quickly identify problem areas and potential problem areas. They also provide a summary of and a way to analyze data to get a sense of the performance of your overall NetBackup environment. Maintaining a separate database allows Advanced Reporter to retain a record of NetBackup activities long after the NetBackup administrator has purged expired backup information from the NetBackup logs. This historic data allows you to spot trends and trouble.

NBAR consists of the following components:

- A client delivery system that distributes the Java applet GUI to individual browsers.
- The Java applet GUI that is started from a browser.
- A database server for the NBAR database.
- A data collection service.
- A configuration utility.

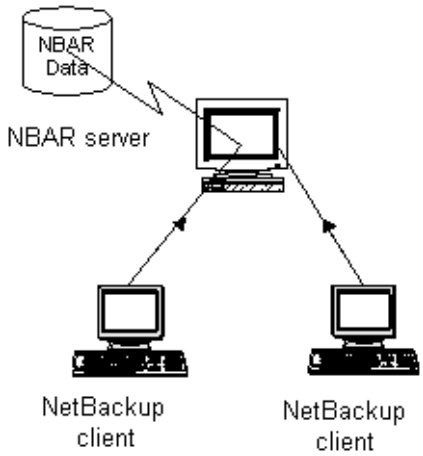
NBAR

In the basic NBAR configuration, NBAR is installed on a NetBackup Data Center master server. The NBAR database server resides on this master server, as do the configuration utility and the client delivery component. NBAR gathers information about the NetBackup environment by running NetBackup commands. NBAR then loads the information gathered into its database. The process that collects this data is called the *loader*.

Timing of Data Loader

The data loader runs at 7:00 a.m. daily by default. This means that at 7:00 each day, NBAR's collection process copies data from the NetBackup database to the NBAR database. If you want to schedule the data loader to run at a different time, or more often, you can do so through the configuration utility. See "Modifying Configuration Information" on page 129 for more information on how to use the configuration utility. Ideally, the data loader will run at a time or times when there is little NetBackup activity on your system. This way the data collected will be as complete as possible. The data loader will only capture jobs that have completed. Jobs that are still in progress will be captured the next time the loader is run.

NBAR configuration



Data Load in Progress Icon

In NBAR 4.5, you can configure the data loader to run more than once a day. If a user generates a report while the data loader is in progress, the data load in progress icon appears. This icon indicates that the information in the reports may not be completely accurate because NBAR is in the process of collecting data. If a report is on display when the loader finishes loading collected data, NBAR automatically regenerates the report with the up-to-date information.

If you are in a GDM environment, the icon only displays if you are generating reports on the managed server on which the data loader is active. No icon displays when you generate GDM reports or reports for a managed server on which the data loader is not active.

Click the toolbar button to display a tooltip estimating the total time for data loader activity. The average total times are based on historic times for loader activity.

NBAR in a GDM environment

Note You must have already configured your NetBackup servers for GDM. If you have not already done so, please refer to the NetBackup *System Administrator's Guide* for information. For instructions on how to add a GDM machine to bp.conf, you can refer to "Allowing NBAR Access to GDM Data" on page 192 of this manual.

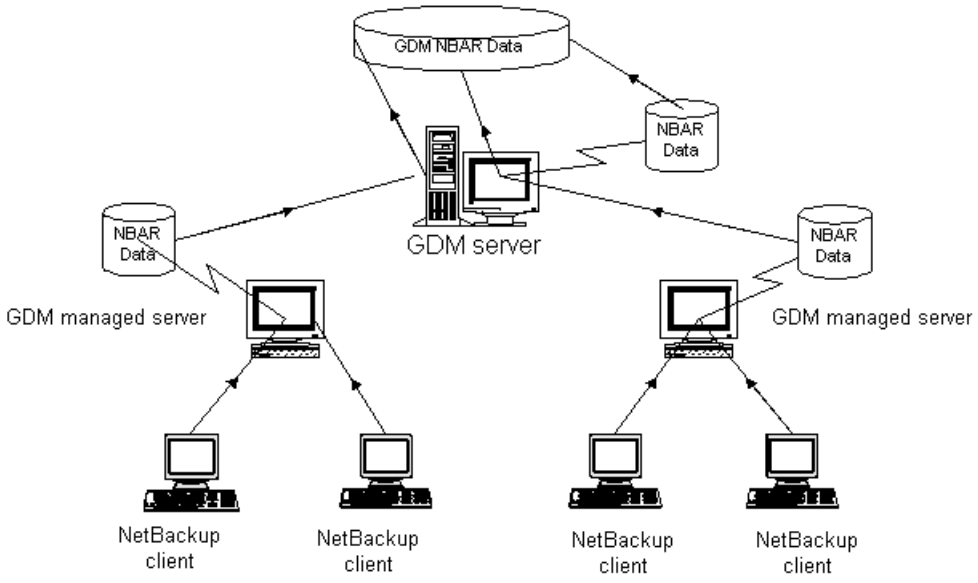
NBAR in a GDM environment has all the functionality of NBAR, with the added ability to report on multiple NetBackup master servers. This feature moves the NBAR product from a single server architecture to a multi-server architecture. Using NBAR in a GDM environment allows you to gain perspective on the health of your global NetBackup system. GDM reports answer important questions like, which master server has the fastest growing catalog, which master server has the most problems with its backup jobs, which master servers are backing up the most data, which storage units are likely to need to recycle their media the soonest, and how long the rollup took for each server that is part of the GDM domain. These reports provide an overarching view of all the systems that are part of a GDM domain.

In this configuration, the NBAR server components must reside on a NetBackup GDM master server and on every NBAR server managed by this GDM master. These components include:

- The client delivery system which delivers the Java GUI applet to a browser,
- The database server,
- Data collection services,
- The configuration utility.

Note In this documentation NetBackup master servers with NBAR installed are called *GDM managed servers*. The GDM master server with NBAR installed is called the *GDM server*. Formerly, the GDM server was known as the *Master of Masters*, or MoM.

NBAR configuration in a GDM environment



In a GDM environment, each NBAR managed server still gathers NetBackup information from the system on which it is installed. This information is loaded into the local database server and summary information for the GDM reports is delivered to the GDM database tables on the GDM server.

Once in each 24-hour period each GDM managed server compiles information from the local NBAR database and sends the data to the GDM master server. The process of collecting the data and passing it to the GDM master server is called a *rollup.*

Timing Data Collection

The data loader runs at 7:00 a.m. daily by default. This means that at 7:00 each day, NBAR's collection process copies data from the NetBackup database to the NBAR database on each GDM managed server. The data loader will only capture jobs that have completed. Jobs that are still in progress will be captured the next time the loader is run.

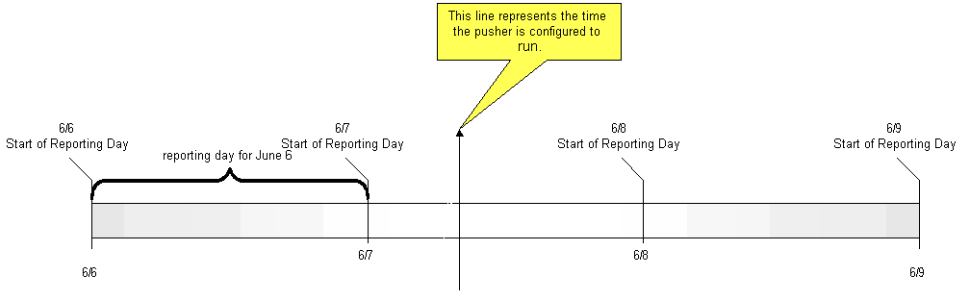
In addition to the data loader, in a GDM environment, the administrator must configure two other critically important times for each GDM managed server: the daily rollup run start time and the Start of Reporting Day (SORD) time. These times will determine what NetBackup activity is included in each rollup.

The daily rollup run start time is the time each GDM managed server begins to rollup its data to send to the GDM server. This parameter is set in time local to the GDM managed server, which is not necessarily the same as the time for the GDM server. (The GDM managed server and the GDM server may be in different time zones.) By default, the rollup begins at 7:30 a.m. daily.

The Start of Reporting Day parameter indicates the time at which a new reporting "day" (one 24-hour period) starts for each GDM managed server (in local time). The GDM server uses this time to distinguish what day the job ran (from the perspective of the GDM managed server) when it compiles the rollup information from every GDM managed server.

As a general guideline, for a given 24-hour-period, you should time data collection on each GDM managed server for after NetBackup activity has stopped, and time the rollup to the GDM server later than that.

Timing data collection in NBAR



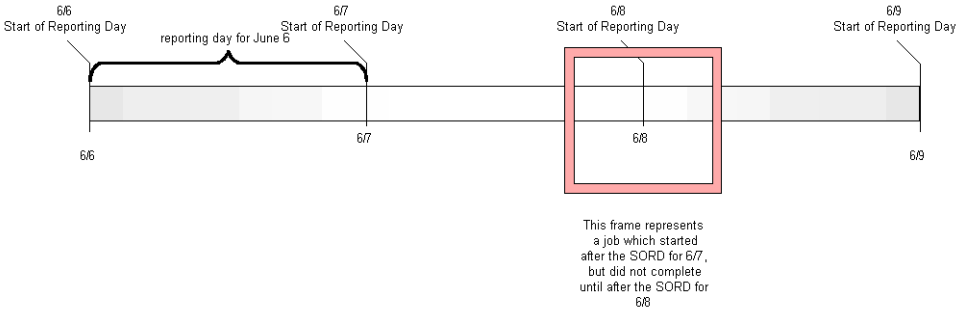
You may be in a situation where data is loaded to the local database before all backup jobs have completed. If you want to be sure to capture the data from all jobs in the next rollup, you must configure the daily rollup time so that it is scheduled well after the SORD.

Caution Do not change the SORD once you have set it. NBAR will not be able to separate one day's data from another's.

How NBAR defines a day

Each GDM managed server defines a 'day', for data collection purposes, as a 24-hour chunk of time. For example, if you define the SORD as 8 am, then the 'day' is 8 am Monday - 7:59 am Tuesday. This GDM managed server day covers parts of two calendar days, but any job which starts before 8 am on a Tuesday is counted towards Monday's activity because it falls within the same 'day' as defined by that server.

Timing jobs in NBAR



Installing NetBackup Advanced Reporter 2

This chapter explains how to install VERITAS NetBackup Advanced Reporter 4.5 (NBAR) on your NetBackup Master server and how to access it from a supported web browser.

You will find separate instructions for UNIX and Windows installations. Each set of instructions contains information for environments with a single NBAR server and for GDM environments (more than one NBAR server).

This chapter also describes how to upgrade from a previous version of NBAR, how to uninstall NBAR for each type of system and describes a little bit about beginning NBAR data collection.

Supported Platforms

There are two parts to platform support: the host operating systems and versions of NetBackup that the server components run on, and the operating systems and browsers that the client components run on.

For more information on supported platforms, please refer to the Product Dependencies section of the NetBackup 4.5 *Release Notes.*

Platform Requirements

- NBAR 4.5 supports NetBackup 4.5 DataCenter.
- NBAR 4.5 does not support BusinesServer or Cluster Server machines.

Supported Server Platforms

NetBackup Advanced Reporter 4.5 supports the following operating systems:

Solaris

Solaris 2.6

Solaris 7

Solaris 8

Note On Sun/SPARC systems.

HP

HP-UX 11.0

HP-UX 11i

Note We strongly recommend you install HP-UX patches PHKL_22840 and PHNE_22397. These patches have dependencies on other patches. Refer to the HP support site at www.hp.com for more information.

Windows

Windows NT 4.0 Workstation with Service Pack 6

Windows NT 4.0 Server with Service Pack 6

Windows 2000 Professional with Service Pack 2

Windows 2000 Server with Service Pack 2

Windows 2000 Advanced Server with Service Pack 2

Windows 2000 Data Center with Service Pack 2

Supported Client Platforms

VERITAS NetBackup Advanced Reporter 4.5 supports the following operating systems and browsers marked with an X:

Operating System	Netscape 4.7x	Netscape 6	Microsoft Internet Explorer 5.5	Microsoft Internet Explorer 6.0
Solaris 2.6 on SPARC stations	X	X		
Solaris 7 on SPARC stations	X	X		
Solaris 8 on SPACE stations	X	X		
HP-UX 11.0	X	X		
HP-UX 11i	X	X		
Windows NT 4.0 Workstation	X	X	X	X
Windows NT 4.0 Server	X	X	X	X
Windows 2000 Professional	X	X	X	X
Windows 2000 Server	X	X	X	X
Windows 2000 Advanced Server	X	X	X	X
Windows 2000 Data Center	X	X	X	X

Browser Versions

- Only a preview release of Netscape 6 was available for testing. On some platforms, the JRE is not installed automatically with Netscape 6. Before running NBAR for the first time, make sure that Java support is enabled, and that the JRE is installed and accessible. To verify that the Java plugin is installed, enter “about:plugins” as a URL in your browser. You should see Java Plugin in the list of installed plugins.
- NBAR requires an English language browser.

Calculating Installation Disk Space Requirements

There are two parts to calculating the amount of disk space you will need. First, you need sufficient disk space to install the software and second, you need enough space to allow NBAR's database to grow.

Disk Space

To install the program, the amount of space you need varies depending on the operating system. Use these figures only as a guide.

Windows Systems

- You need about 50 megabytes free to install the product in the install directory on a server.
- You need about 100 megabytes on the drive where the operating system resides. This is because the Java applet is distributed as a Java distribution unit and requires a lot of space. If there is not enough space on the disk, the Start button for the applet may not appear.

UNIX Systems

- You need about 60 megabytes free to install the product in the install directory on a server.

Database Conversion

If you are upgrading your NBAR installation from NBAR 3.2.1, you will need enough space to perform a database conversion.

- First, you need enough space to save the old database. Plan on space the size of the old database plus ten percent.
- Second, you need temporary space for the conversion. Plan on about 75 percent of the space needed for the old database.
- Third, you need space for the new database. Plan on roughly the same amount of space as the old database required.

Database files are located in the following directories:

On UNIX systems: <*install_path*>/var/nbar

On Windows systems: <*install_path*>\data\nbar

Data Collection for NetBackup before NBAR is Installed

NetBackup Advanced Reporter will load all available NetBackup data. NetBackup retains data based on several settings including the retention of the backup image, the KEEP_LOGS setting, and other NetBackup configuration options.

If on the date NBAR is installed, NetBackup has been running for some time, NBAR may not be able to gather all the data for accurate reporting. For instance, a system may have had a backup with an infinite retention level, but it was completed 60 days ago and the job information is gone. In this case we could gather the image data, but would have no information regarding the NetBackup job that created the image. Another example of this problem would be if a job was completed, and the image is still valid but the policy had been deleted. NBAR has no way to gather policy information from a past configuration. In this case it would be impossible to associate the job with a particular policy.

In order get the most accurate data, we advocate installing NBAR and NetBackup at the same time. This is a best practice. If this practice is not followed, be aware that data on NBAR reports that precedes initial NetBackup Advanced Reporter installation must be interpreted carefully.

We expect data going forward in time from the point of installation to be free of the kinds of accuracy issues explained above.

License Keys

We assume you have a valid license key for NetBackup DataCenter. In addition, you must have a valid license key for NBAR 4.5. If you are planning to install NBAR in a GDM environment, you must have valid GDM license keys for the GDM server and each managed server. For more information about what constitutes a valid key, consult your VERITAS NetBackup documentation.

Finding License Key Information on Windows Systems

On Windows systems, make sure a valid license key for NetBackup Advanced Reporter has been registered. From the NetBackup Administration Console, select the **Help** menu. From the **Help** menu, click **License Keys**. The **License Keys** screen displays current license information and the evaluation period if an evaluation license is installed.

Finding License Key Information on UNIX Systems

On UNIX systems, make sure a valid license key for NetBackup Advanced Reporter has been registered.

Use the command:

<*install_path*>/netbackup/bin/admincmd/get_license_key

to list and add keys.

Planning for a GDM Configuration

If you are planning to run NetBackup Advanced Reporter in a GDM environment, we suggest you take the following steps:

- List all NetBackup Master servers that are part of the GDM domain.
- List the NetBackup Master server that functions as the GDM server (previously, the Master of Masters)
- Each of these machines must:
  - Be running NetBackup 4.5
  - Have NBAR 4.5 installed
  - Have NetBackup, NBAR, and GDM licenses

UNIX Installations

This section contains detailed instructions for installing NBAR on a Solaris or HP-UX server.

Release Materials

The NBAR installation contains the following:

- An install script,
- The files necessary to install this application,
- A copy of this guide in PDF format, and the release notes in HTML format.

Installation Requirements

- You must be a root or super user.
- You must have NetBackup DataCenter 4.5 installed on the master server.
- In order for NBAR to report accurate and complete media information, there must only be one volume database and it must reside on the master server.
- You must be installing on a Solaris machine running version 2.6, 7, or 8, or an HP-UX machine running 11.0 or 11i.
- You must have a valid evaluation or permanent NBAR license key.
- If you are installing in a GDM environment, you must have valid GDM license keys for the GDM server and each managed server. NetBackup must be configured for GDM.
- The installation directory must have sufficient space for the NBAR installation.

Notes about Installation

The default installation directory is `/opt/VRTSnbaro` for Solaris systems, and `/usr/openv/nbar` for HP-UX systems.

Caution We do not recommend nor support installation into a directory beneath the default directory, for example, `/opt/VRTSnbaro/nbar`.

In general, it is not a good idea to install into the partitions on which the `/tmp` or `/` (root) directories reside.

Advanced Reporter runs under its own user name and user group. The defaults are nbar and vrts.

The database server requires a TCP port. The default port is 3306. The default port number is registered to MySQL with the Internet Assigned Numbers Authority (http://iana.org).We suggest you use the default port unless it is already in use.

The httpd (web) server, which is the client delivery component, also requires a TCP port. The default port is 8885. We suggest you use the default port unless it is already in use.

We strongly suggest you seed the database during the installation procedure. The database then will be populated with all available NetBackup data.

Note The initial seeding may take a significant amount of time if you have a large number of clients under NetBackup control. You can choose not to seed the database at install time.

Advanced Reporter requires that its database is updated at least once a day. This is achieved through a loader script, arloader.sh. By default, the installation program configures the loader to run at 7:00 a.m.

The same installation script is used for GDM installations and non-GDM installations. Refer to the sections below for instructions on how to handle this part of the installation.

Installation Procedure

▼ To install NBAR on a UNIX server:

1. Log in as the root user on the master server.

   If you are already logged in, but are not the root user, execute the following command:

   su - root

2. Make sure a valid license key for NetBackup Advanced Reporter has been registered.

   Use the command:

   <install_path>/netbackup/bin/admincmd/get_license_key

   to list and add keys.

3. Insert the CD-ROM containing the Advanced Reporter software in the drive.

4. Change your working directory to the CD-ROM directory:

   `cd /<cd_rom_directory>`

   where <*cd_rom_directory*> is the path to the directory where you can access the CD-ROM. On some platforms, it may be necessary to mount this directory.

5. To install NetBackup Advanced Reporter, execute the following command:

   `./install`

   Because other NetBackup products are included on the CD-ROM, a menu appears.

6. Select **NetBackup Add-On Product Software**.

   a. Select the **NetBackup Advanced Reporter** option.

   b. Enter **q** to quit the menu.

   c. When you are asked if the list is correct, type **y**.

7. Follow the prompts in the install script to complete the installation.

8. You will be asked if you want to change the default configuration for GDM.

   - If you are not installing in a GDM environment, accept the defaults and choose option 3. This option tells the install script that this server is not configured for GDM.

   - If you are installing in a GDM environment, answer yes and follow the instructions.

     - If the machine on which you are installing will be the GDM server, choose option 1.

This means that this machine will be the master of masters. A GDM license is required on this machine, and a KNOWN_MASTER entry is required in this server's bp.conf file for each server that is part of this server's GDM domain.

For more information on GDM configuration, refer the NetBackup *System Administrator's Guide*.

- If the machine on which you are installing will be a GDM managed server, choose option 2.

  This means that this machine will be part of a GDM domain. You must know the name of the GDM server and the number of the TCP port for the NBAR database to the GDM server.

As the script runs, it produces progress messages. When the installation is complete, the script will provide a summary of the installation.

To run the NetBackup Advanced Reporter Java applet from your web browser, use the following URL:

`http://<host>.<domain>:<port>/nbar.html`

Upgrading from NBAR 3.2.1 to NBAR 4.5

To upgrade NBAR from 3.2.1, you must first uninstall NBAR following the instructions below, and then reinstall the product.

Due to changes in NBAR's database format with release 3.4, when you upgrade NBAR from 3.2.1, the installation performs a database conversion. During installation, the amount of disk space required to accomplish this task will be displayed. You will be asked for the names of two temporary directories that the database conversion utility will use. You can choose any directories, as long as they have at least as much space as the installation script indicated was required.

Caution To preserve historical NBAR data, you must install to the directory where the previous version of NBAR was installed.

When NBAR is uninstalled, the NBAR historical data in the database files will be collected and preserved in the file `<tmpdir>/VERITASnbar-db.tar.Z`. During the installation process, the data in this file is provided to the new database. When you are certain that your new NBAR installation is running correctly, you can delete this file.

Note You must close any browser windows that are running NBAR after you have performed an upgrade, and restart the browser. This process will help the browser install the new NBAR applet plugin.

Upgrading from NBAR 3.4 to NBAR 4.5

To install NBAR 4.5, you must first uninstall NBAR 3.4.

Note You must close any browser windows that are running NBAR after you have performed an upgrade, and restart the browser. This process will help the browser install the new NBAR applet plugin.

Uninstalling NetBackup Advanced Reporter

▼ To uninstall NetBackup Advanced Reporter from a UNIX server:

1. Log in as the root user on the master server.

   If you are already logged in, but are not the root user, execute the following command:

   su - root

2. Execute the uninstall command or script:

   - On a Solaris server, type:

     pkgrm SUNWnbaro (for versions of NBAR prior to 4.5)

     pkgrm VRTSnbaro (4.5 only)

   - On an HP-UX server, type:

     <install_path>/netbackup/bin/install_nbar -deinstall

     where <*install_path*> is the directory in which NetBackup resides.

3. When the uninstall command or script finishes, it will mention several temporary files that may have been created.

   If this is a complete uninstall, rather than a step in the upgrade process, you may delete these files.

   If you are upgrading or reinstalling, leave these files until after the installation (see "Installation Procedure", above) has completed.

   These are the files you may find:

   <*tmpdir*> / VERITASnbar-db.tar.Z

   <*tmpdir*> / VERITASnbar-env.sh

<*tmpdir*> / VERITASnbar-VRTSnbaro-crontab.<*PID*>.r (optionally created)

where <*tmpdir*> is the value of the TMPDIR environment variable at the time the install script is executed, and <*PID*> is the value of the process ID of the script.

Windows Installations

This section describes how to install NBAR on a Windows system. It also describes how to upgrade or uninstall the product.

Release Materials

The NBAR installation contains the following:

- A setup program,
- The files necessary to install this application,
- A copy of this guide in PDF format and the release notes in HTML format.

Installation Requirements

- You must have administrator rights on the local machine.
- You must be running Windows NT 4.0, Service Pack 6 or greater, or Windows 2000, Service Pack 2.
- You must have NetBackup Master 4.5 installed on the machine where you want to install NBAR.
- In order for NBAR to report accurate and complete media information, there must only be one volume database and it must reside on the master server.
- You need about 50 megabytes free to install the product in the install directory on a server.
- You need about 100 megabytes on the drive where the operating system resides. This is because the Java applet is distributed as a Java distribution unit and requires a lot of space. If there is not enough space on the disk, the Start button for the applet may not appear.
- You must have a valid evaluation or permanent NBAR license key.
- If you are installing NBAR in a GDM environment, you must have a valid GDM license key.
- You must have sufficient room on the system for the NBAR application and for the database.
- If you want to use Microsoft Internet Explorer to access NBAR, you must have it installed and configured on your system before you install NBAR.

- You must have Microsoft Internet Information Server (IIS) 4 or higher running on an NT 4.0 server, Microsoft Peer Web Services (PWS) running on an NT 4.0 workstation, or Microsoft Internet Information Services 5 running on a Windows 2000 machine.

Notes about Installation

- You can install Advanced Reporter on any server which has NetBackup Master 4.5 installed. The default installation directory is

  `c:\Program Files\VERITAS\NetBackup Advanced Reporter`.

Caution We do not recommend nor support installation into a directory beneath the default directory, for example, `c:\Program Files\VERITAS\NetBackup Advanced Reporter\nbar`.

- You have an opportunity to correct information about the server where NBAR will be installed. You must enter the name of the server (host name), and the complete domain name (DNS suffix).
- The database server requires a TCP port. The default port is 3306. The default port number is registered to MySQL with the Internet Assigned Numbers Authority (http: / /iana.org).We suggest you use the default port unless it is already in use.
- The http: port number for the IIS server also requires a TCP port. The installation reads the port number from the registry. The default port number is 80. Only change this port number if you know that the web server is configured to use a different port. Changing this number will not change the configuration of the web server.
- We strongly suggest you populate the database during the installation procedure. The database will be seeded with all available NetBackup data.

Note The initial seeding may take a significant amount of time if you have a large number of clients under NetBackup control. You can choose not to seed the database at install time.

- Advanced Reporter requires that its database is updated at least once a day. This is achieved through a loader script, arloader.bat. By default, the installation program configures the loader to run at 7:00 a.m.

For GDM environments only

- The installation program will also contain a GDM Configuration Settings screen.
  - If you choose not to configure this NBAR server for GDM, nothing further is required.

- If you choose to configure this server as the GDM server, a GDM license is required. In this case, this server will receive reporting information from all NBAR servers in the GDM domain.
- If you choose to configure this server as an NBAR server that is a member of a GDM domain, a GDM license is required. In this case, reporting information from this server will be sent to a GDM server. You must also provide the fully-qualified name of the GDM server and the MySQL port for the GDM server.

Note The GDM server must already have NBAR installed and a GDM license. However, if you have not already configured your NetBackup GDM domain, you can do so after you have installed NBAR on your GDM machines.

Installation Procedure

▼ To install NetBackup Advanced Reporter 4.5 on a Windows server:

1. Log in with administrative rights.
2. Insert the CD-ROM that contains the NetBackup server software.
   - On systems with AutoPlay enabled for CD-ROM drive, the setup program will start automatically.
   - On systems that have AutoPlay disabled, run `Launch.exe` from the root directory.
3. On the NetBackup Install browser, click the **Additional Products** link in the left column. The main window updates and enables you to install additional products or view documentation.
4. Click the **Additional Products Installations** link. The browser refreshes and displays the current list of products available for installation.
5. Click the **Advanced Reporter** link.
6. The first screen you will see is the standard InstallShield Welcome screen. Click **Next** and follow the prompts to complete the installation.

Note If IIS 4 is installed, the installation process will start the Web Publishing Service if it is not already started. If PWS is installed, the installation process will restart the Web Publishing Service. If IIS 5 is installed, the installation process will start it.

7. The final screen reviews the information you have entered. If you wish to change any of it, click **Back**. Otherwise, click **Next** to begin copying the Advanced Reporter files.

8. When the installation is complete, a log file displays the output from `arconfig`. If you want to change any of the settings, you must run arconfig again.

   For more information on arconfig, please refer "Modifying Configuration Information" on page 169.

9. When the installation has completed, you will have the opportunity to view the Release Notes and to start the application.

Upgrading from NBAR 3.2.1 to NBAR 4.5

The installation process will detect the 3.2.1 installation and ask you if you want to upgrade (which will preserve the database information) or perform a clean install (which will delete database information). Both choices will delete the 3.2.1 installation.

The upgrade creates a copy of the NBAR 3.2.1 database in the `<install-directory>\nbar_olddb` directory, which might be, for example:

```
c:\Program Files\VERITAS\NetBackup\NetBackup Advanced
Reporter\nbar_olddb
```

After you run NBAR and confirm that the data has been properly migrated, you may delete the `nbar_olddb` directory to recover the disk space. You can verify that the data has been migrated by viewing reports from a time period predating the upgrade.

Upgrading from NBAR 3.4 to NBAR 4.5

The installation process will detect the 3.4 installation and ask you if you want to upgrade (which will preserve the database information) or perform a clean install (which will delete database information). Both choices will delete the 3.4 installation.

Note You must close any browser windows that are running NBAR after you have performed an upgrade, and restart the browser. This process will help the browser install the new NBAR applet plugin.

Note If you want to reinstall version 4.5, you must first uninstall it using Add/Remove Programs.

Uninstalling NetBackup Advanced Reporter

- Use the Add/Remove Programs utility in Windows to uninstall NBAR.

Starting the Java Applet GUI for the First Time

Now that you've completed the installation process, you can launch NBAR's Java applet GUI.

When you start Advanced Reporter for the first time, the application will install itself as an extension to your browser and run as a Java plug-in. The first thing that you will see will be a security message from your browser indicating that a request is being made to install a plug-in onto your workstation. Click **Yes** to accept the installation. Your browser may be inactive for a few moments while the plug-in is installed. If you are using Microsoft Internet Explorer, Advanced Reporter starts at this point. Netscape Navigator users must exit the browser completely and restart it before Advanced Reporter will work.

Note If a new version of the plug-in is detected, it will automatically install on your web browser. Selecting the optional **Remember This Decision** checkbox will prevent the security messages from displaying during subsequent updates. If you want to remove the Java applet, please refer to your browser's documentation for information on how to remove a plug-in.

Running the Java Applet GUI

- To access NBAR 4.5 installed on a UNIX system, use the following URL from your web browser:

  http://<*host*>.<*domain*>:<*port*>/nbar.html

Note The default port is 8885.

- To access NBAR 4.5 installed on a Windows system, use the following URL from your browser:

  http://<*host*>.<*domain*>/nbar/nbar.html

Note If the port number of the web server is set to something other than 80 (the default), you must specify the port number in the URL. The syntax is:
http://<*host*>.<*domain*>:<*port*>/nbar/nbar.html

We suggest you add the Advanced Reporter program URL as a **Bookmark** or **Favorite** for easy access.

Introduction to the NBAR Reports 3

This chapter describes how to use NBAR to view reports.

After reading this chapter you will be able to:

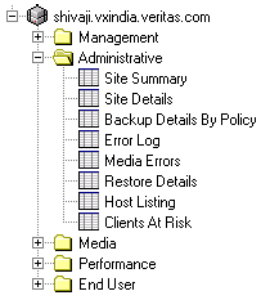
- Navigate the interface
- Adjust the report display
- Change the reference date
- Change the reporting timeframe
- Print selected reports

Exploring the Java Applet GUI

The Advanced Reporter user interface is a Java-based interface that allows users to select and view a variety of *Management*, *Administrative*, *Media*, *Performance*, and *End User* reports.

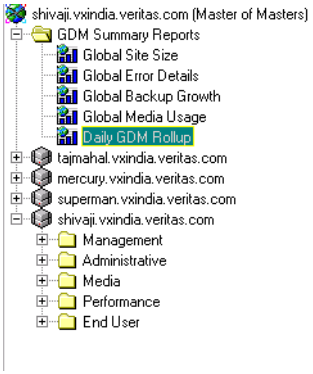
The interface displays a window that contains left and right panes with built-in navigation tools. These are described below.

NetBackup Advanced Reporter Console Tree - Non-GDM version



Note If you have the optional GDM add-on to NetBackup, you will also see GDM summary reports in the NBAR console tree.

VERITAS NetBackup Advanced Reporter Console Tree - GDM version



How to Navigate in the Advanced Reporter Interface

There are several features in the GUI that make it easier to move around and understand the Advanced Reporter interface. These features include a toolbar, a menu bar, tool tips, and history and status lines.

What Do Toolbar Buttons Do?

The toolbar provides shortcuts for some actions and allows you to move between reports conveniently. When the cursor hovers over a Toolbar button, a tool-tip appears describing the function of the button.

One of the toolbar buttons, the Data Load in Progress button, displays only if both these conditions are met: the console is not displaying a GDM report, and the data loader is active for the master server for which the report is being displayed.

Toolbar Icons	Tool Tip	Tool Function
	New reports browser	This tool displays a new Advanced Reporter window. This feature makes it easier to compare reports.

Toolbar Icons	Tool Tip	Tool Function
	Change Advanced Reporter's Reference Date.	This tool displays the Edit Reference Date dialog box. For details on this dialog box, refer to "How Do I Change the Reference Date?" on page 65.
	Change the report's time frame	This tool displays the Edit Report's Timeframe dialog box. For details on this dialog box, refer to "What Determines the Timeframe for a Report?" on page 67.
	Copy to clipboard	This tool creates a copy of the report currently being viewed and places it in your computer's clipboard.
	Print report	This tool brings up the Print dialog box.
	Show / hide sidenotes	This tool allows you to show or hide the side notes that display to the right of the GDM reports. **Note** This toolbar button will only display on GDM servers.
	Help Topics	This tool displays the *NetBackup Advanced Reporter System Administrator's Guide* in a separate browser window.
	Data load in progress	This tool displays if the data loader is active. If you run reports when the data loader is in progress, the results may not be completely accurate. **Note** This toolbar button will only display when the data loader is running.
	Previous report	This tool displays the previously displayed report. **Note** This button is only available after you have generated more than one report.
	Next report	This tool displays the next report from the history list. **Note** This button is only available after you have generated more than one report and used the **Previous Report** button.

What Does the Report History Drop-Down Box Tell Me?

The report history window appears at the top of each window to the right of the toolbar and displays the name of the report that is currently in the right pane.

Report History Drop-Down Box

Use the arrow to the right of the drop-down box to select any previously viewed report in the current viewing session. This is a quick way to access the desired report without having to page through each of the previous reports over again.

What Can I Do with the Menu Bar?

The menu bar appears at the top of each window above the toolbar. The menu choices are described below.

Menu	Entries
File	New Browser, Print, Close
Edit	Copy, Reference Date, Timeframe
View	Next, Previous, Clear, Show / Hide Sidenotes (for GDM reports)
Reports	Displays a list of reports organized in folders and subfolders. Name of each connected server, including a GDM summary reports entry if GDM is running. You can access individual reports for each server from here.
Help	Release Notes, Help Topics, NetBackup Trouble Shooting Guide, VERITAS on the Web, About VERITAS NetBackup Advanced Reporter

What Does the Window Adjustment Bar Do?

The window adjustment bar sits between the left and right panes of the Advanced Reporter window. From the default position in the middle of the screen, the arrows at the top move the bar either fully to the left, exposing only the right pane, or fully to the right, exposing only the left pane. To adjust the window size:

- Click on the top arrow with the left mouse button to move the window bar to the left of the screen, or click on the bottom arrow to move the window bar to the right of the screen; or,
- Position the cursor over the window bar. You will know if it is in the right place when you see a **left-right** arrow appear. Then click the mouse button and drag the bar to the desired location.

What Does the Status Line Tell Me?

The status line appears at the bottom of each window and displays the status of the current task.

The Status Line

Note The status line may also indicate a Java-related problem. If this occurs, you must exit NBAR and the web browser, then restart the web browser and reload the NBAR application. If you encounter recurring problems using NBAR, or with the NBAR user interface, please refer to “Getting Help” on page xx.

Understanding the Left and Right Display Panes

The Java applet GUI is composed of two panes, a left pane that holds the report tree, and a right pane that displays the reports.

Where Is the Advanced Reporter Report Tree?

The console tree appears in the left pane during a VERITAS NetBackup Advanced Reporter 4.5 session. You can hide the tree to obtain a larger report display area. You can generate all reports from either the left or right panes. The reports are organized into five (six, if GDM is enabled) categories, each represented by a folder. These are:

- **Management** reports

The management reports are further grouped into lower level folders (**Full Backups**, **Incremental Backups**, **Restore Jobs** and **Catalog Usage** as well as two stand-alone **Error Log** reports)

- **Administrative** reports

  These reports provide details on backup policies, jobs by site, and error occurrence.

- **Media** reports

  These reports provide information on the status of backup media.

- **Performance** reports

  The performance reports provide information on active policies, drive throughput, and the length of backup windows.

- **End User** reports

  There is only one end user report. It contains the backup history for a particular client.

- If **GDM Summary** reports are present, they have a separate folder.

  The GDM summary reports consolidate information about all of the NBAR servers.

Report folders may appear closed () or open (). To open a folder, position the cursor on the folder and double-click the left mouse button, or click once on the **+** symbol to the left of the folder. The icons for the individual reports appear slightly different depending on whether the report is represented textually or with graphics.

❖ To generate a report from the report tree, position the cursor on the desired report and click the left mouse button. NBAR generates and displays the selected report using the report's default time frame.

Note For more information about the default time frame, see "What Determines the Timeframe for a Report?" on page 67.

The fully-qualified name of the NBAR server that generates the report appears in the upper left corner of each report run in a GDM configuration.

How Do I Display the Context-Sensitive Menu in the Tree?

❖ To display the context-sensitive menu for any report, highlight the report and right-click. A menu containing the following options displays:

- **Open in New Window**

  This option brings up the same report in a new browser window. The reference date remains the same.

- **Reference Date**

This option brings up the Edit Reference Date dialog box.

- **Help Topics**

  This option brings up the *System Administrator's Guide.*

In a GDM configuration only, if you right-click on a folder containing a group of reports, the **Open in New Window**, **Reference Date** and **Help Topics** options are available.

Report Display Area

The right pane is where Advanced Reporter displays all reports. As Advanced Reporter generates each report, the new report appears on top of the previous report. All reports generated during a session remain available in the right pane during the session unless you select **Clear** from the menu. You can also choose to display a report in a new window by opening the **File** menu and choosing **New Browser**. The reference date remains the same.

Note If you have used the **Next Report** or **Previous Report** buttons during the current session, any newly generated reports will appear *after* the last generated report. For example, if you have generated four reports and have used the previous report button to return to the second report generated, the report you generate next will still appear after the fourth report, not after the second.

Hover Labels

If you allow the cursor to linger over a data point, bar, or column heading on one of the NBAR reports, a hover label will display, containing additional data about the data point or column heading.

How Do I Move Through the NBAR Reports?

VERITAS NetBackup Advanced Reporter 4.5 reports have a number of common features. Becoming aware of these features will help you get the most out of the reports.

These features include being able to:

- Use the context-sensitive menu
- Follow report links
- Use dynamic report selection criteria options
- Edit the reference date

- Adjust the reporting time frame

How Do I Display the Context-Sensitive Menu?

❖ To display the context-sensitive menu for any report, right-click anywhere in the report except on a column header. A menu containing the following options displays:

- **Next**

  This option is only available if you have generated more than one report and you are not looking at the most recently generated report. It will display the report generated directly after the report you are viewing.

- **Previous**

  This option is only available if you have generated more than one report. It will display the report generated directly before the report you are viewing.

- **Clear**

  This option clears all report data from the screen. If you have generated many reports, this is a quick way to dispel extraneous information. To view the report you were on when you used the **Clear** command, you must first view another report, then return.

- **Timeframe...**

  This option brings up the Edit Report's Timeframe dialog box.

- **Copy**

  This option copies the text of the currently displayed report. You can paste the data into another format, such as an email or a spreadsheet format. Note that this action does not preserve the name of the NBAR server from which you generated the report.

- **Print...**

  This option brings up the standard Print dialog box.

- **Hide Sidenotes...**

  This option is only enabled for the GDM reports. It allows you to turn off the report sidenotes, which creates more space for the report data.

Note These options are also available from the menu bar or from the toolbar.

- **Properties**

  For certain reports, you can access Job Properties or Policy Properties dialog boxes from the context-sensitive menu. These are mostly administrative reports. The description of the individual report tells you if the feature is present. Access this feature by highlighting a row in one of these reports and right-clicking.

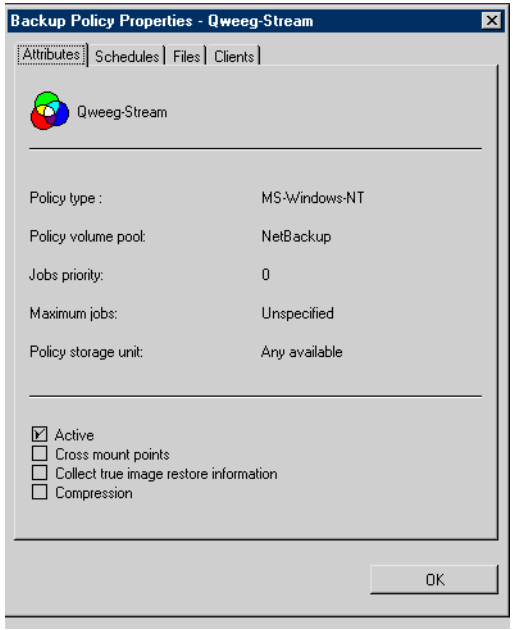
  Below is a description of each property tab.

What Information Do I Get from the Policy Properties Dialog?

You can access the Policy Properties dialog box from the *Backup Details by Policy, Active Policy Definitions*, and *Windows Utilization* reports. The Policy Properties dialog has four tabs: Attributes, Schedules, Files, and Clients. The tabs are depicted below.

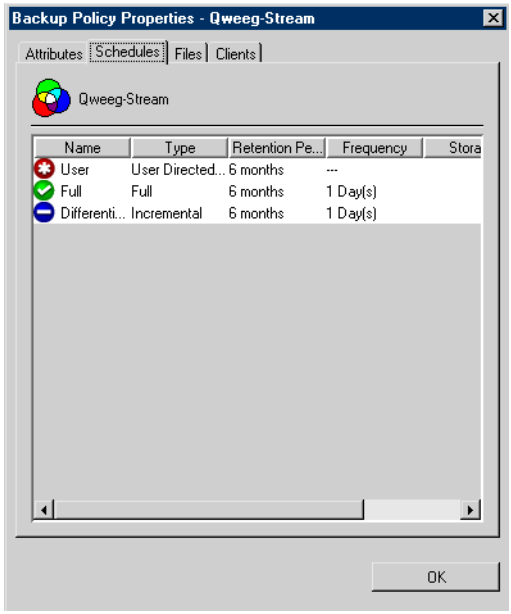
The Attributes tab displays the most pertinent attributes of the policy under analysis. These attributes are assigned through NetBackup.

Policy Properties Dialog - Attributes Tab



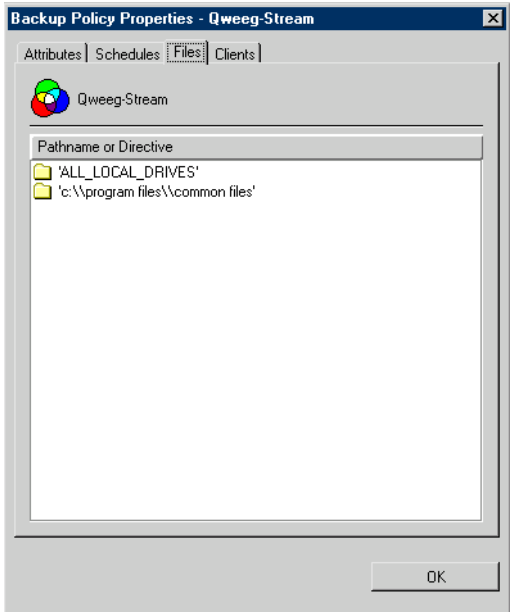
The Schedules tab displays information about the schedules for this policy.

Policy Properties Dialog - Schedules Tab



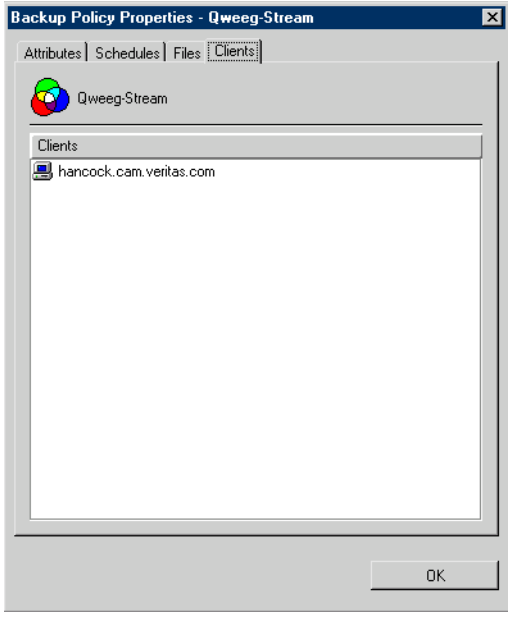
The Files tab displays information about the files backed up by this policy. Some jobs that end with an error may not display pathnames. All this indicates is that the data loader was unable to locate path information for the job because of the way NetBackup stores the information.

Policy Properties Dialog - Files Tab



The Clients tab displays the name of the clients that are part of this policy.

Policy Properties Dialog - Clients Tab

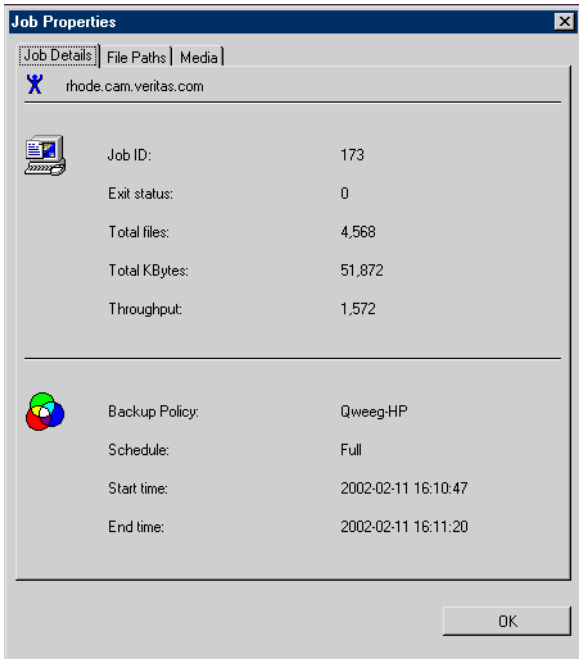


What Information Do I Get from the Job Properties Dialog?

You can access the Job Properties dialog box from the *Site Details Job List*, *Job Details for Policy*, *Restore Details*, and *Client Job History* reports. The Job Properties dialog has three tabs: Job Details, File Paths, and Media. The tabs are depicted below.

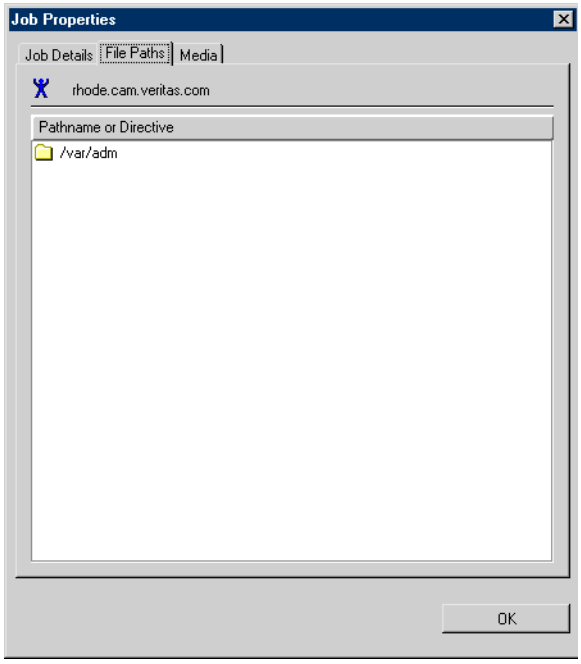
The Job Details tab contains basic descriptive information about the job, such as the job ID and the exit status of the job.

Job Properties Dialog - Job Details Tab



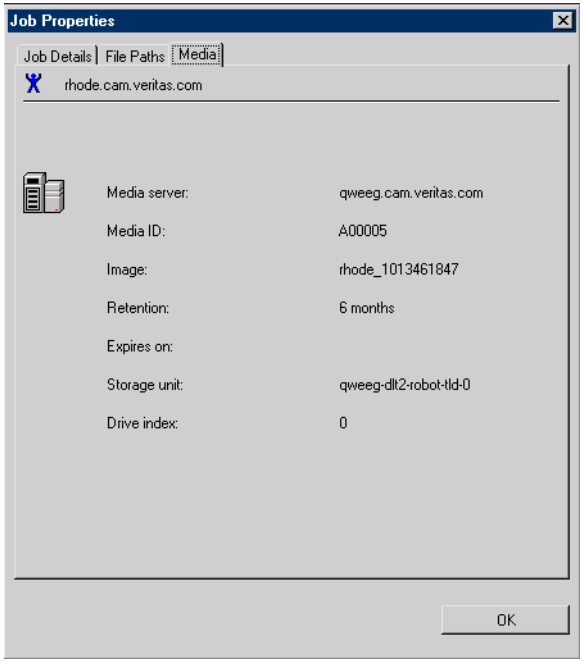
The File Paths tab contains information on the file paths backed up by this job.

Job Properties Dialog - File Paths Tab



The Media tab contains information about the media used for this job, such as the name of the storage unit, the media server and the image.

Job Properties Dialog - Media Tab

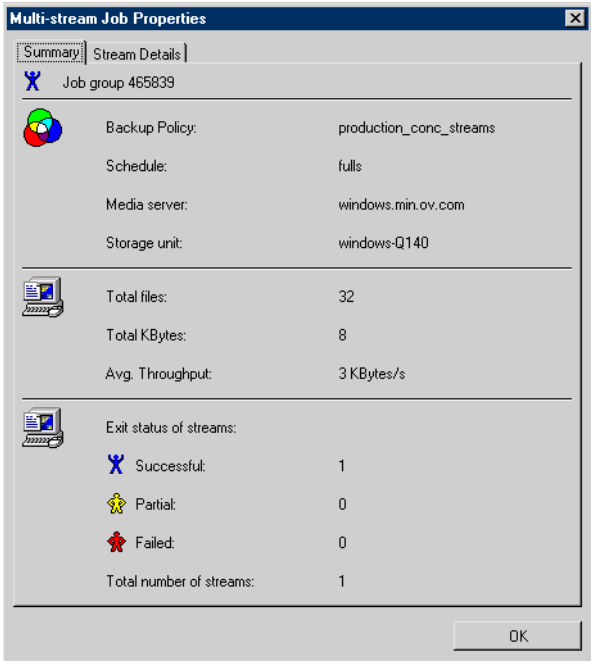


What Information Do I Get from the Multistreamed Job Properties Dialog?

You can access the Multistreamed Job Properties dialog box from the *Site Details Job List*, *Restore Details*, and *Client Job History* reports. The Multistreamed Job Properties dialog has two tabs: Job Details, and Media. The tabs are depicted below.

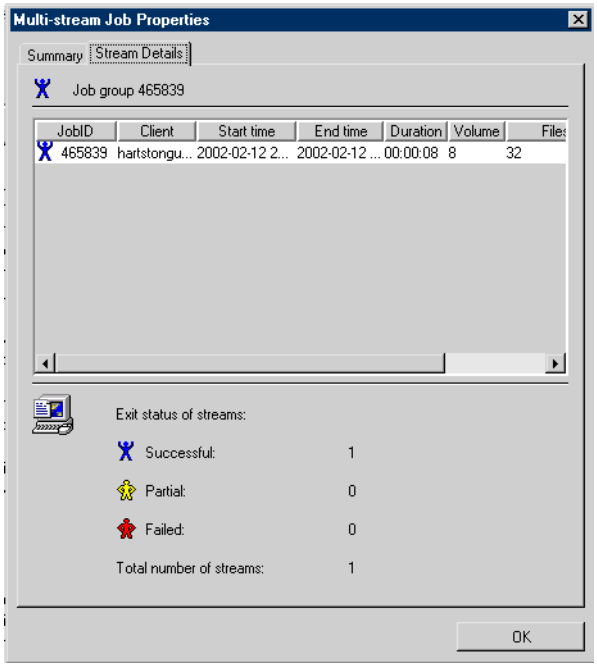
The Job Details tab contains basic descriptive information about the multistreamed job, such as the job group and the exit status of individual job streams.

Multistream Job Properties dialog - Job Details tab



The Media tab contains detailed information about each data stream, such as duration and status.

Multistream Job Properties - Stream Details tab



How Do I Follow Report Links?

Report links are available in many Advanced Reporter reports. They provide access to a related report which provides more detail for the selected NBAR server or time period. A report link may be accessed through a bar on a chart, a field entry in a report, or section sub-title.

For example, the *Full Job Completion Status* report provides details on all full backup jobs run in the last 28 day period. Clicking on the bar that represents one day will link to the job details report for the selected day.

If you link to, or “drill down” to a report from another report, the report that you have linked to will display the same time frame as the initial report.

Note Certain reports are accessible only through report links. These reports do not appear in the report tree in the left pane. The chapter on Miscellaneous reports describes the content of these linked reports.

How Can I Compare Reports?

Advanced Reporter facilitates your ability to compare reports. While you display one report, from the **File** menu, select New Window. Another instance of the browser will come up, allowing you to display another report. The reference date will remain the same. Size the browser windows so that you can compare the reports.

How Do I Use the Dynamic Report Selection Criteria Options?

The Dynamic Report Selection criteria box appears as part of some reports. This box gives you the opportunity to further narrow the focus of the report, usually by specifying particular media servers.

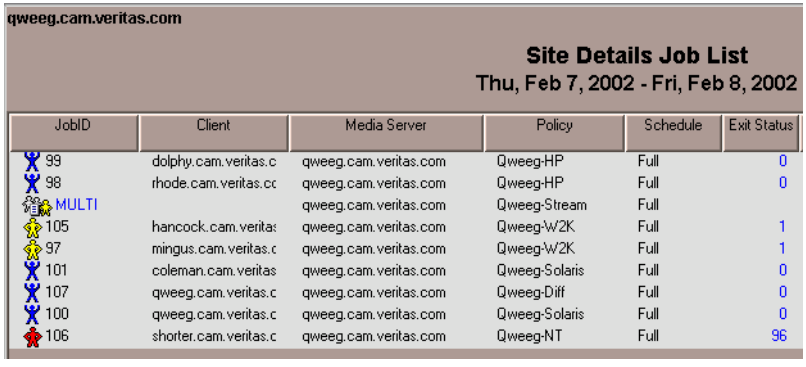
Dynamic Report Selection Criteria box

In this example, you select the name of the media server in the **Select media server** scroll box. Once you have selected a particular media server, click the **Run** button to display the report.

What Do the Icons Next to Entries on Some Reports Mean?

Some reports provide a snapshot of success or failure in the form of an icon next to each entry. A red icon indicates failure. A yellow icon indicates partial success. A blue icon indicates success. An icon with the word MULTI next to it indicates a multistreamed job.

Section of Site Details Job List



qweeg.cam.veritas.com

Site Details Job List
Thu, Feb 7, 2002 - Fri, Feb 8, 2002

JobID	Client	Media Server	Policy	Schedule	Exit Status
99	dolphy.cam.veritas.c	qweeg.cam.veritas.com	Qweeg-HP	Full	0
98	rhode.cam.veritas.cc	qweeg.cam.veritas.com	Qweeg-HP	Full	0
MULTI		qweeg.cam.veritas.com	Qweeg-Stream	Full	
105	hancock.cam.veritas	qweeg.cam.veritas.com	Qweeg-W2K	Full	1
97	mingus.cam.veritas.c	qweeg.cam.veritas.com	Qweeg-W2K	Full	1
101	coleman.cam.veritas	qweeg.cam.veritas.com	Qweeg-Solaris	Full	0
107	qweeg.cam.veritas.c	qweeg.cam.veritas.com	Qweeg-Diff	Full	0
100	qweeg.cam.veritas.c	qweeg.cam.veritas.com	Qweeg-Solaris	Full	0
106	shorter.cam.veritas.c	qweeg.cam.veritas.com	Qweeg-NT	Full	96

How Do I Change the Reference Date?

This feature changes the reference date for all reports for this Advanced Reporter session. The reference date is the last day of the time frame, or reporting period, for any Advanced Reporter report. The default reference date is today's date, that is, the date of the day you are running NBAR reports.

Note The time field in the reference date defines a boundary of an NBAR day. For example, if the reference date is set to Feb 11 2002 11:00 AM, then the NBAR day will start on Feb 10 2002 11:00 AM and will end Feb 11 2002 at 11:00. NBAR will consider all information falling between Feb 10 at 11:00 AM and Feb 11 at 11:00 AM Feb 10 data.

In general, the reports reached through drill-down from another report retain the reference date of the first report. If you open a new browser window, for example, to compare two different reports, the reference date you set will carry over to the new window as well.

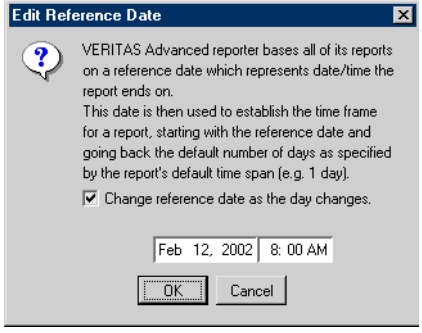
Exceptions to this are reports for which only current data are relevant. For example, if you are using the previous day as a time frame for the *Global Site Size* report, and you drill-down to the *Active Policy Definitions* report, the date for the *Active Policy Definitions* report will be the date you are running the report. This is because current data is the only data that is relevant when determining which policies are active.

▼ To change the reference date:

1. Choose **Reference Date** from the **Edit** menu.

   The Edit Reference Date dialog box appears.

The Edit Reference Date Dialog



2. Select a new date for the last day of the reporting period.

Adjust the date and time by clicking on each part of the date to highlight it and using your keyboard's up arrow or down arrow, or typing in the new date or time.

3. Examine the **Change reference date as the day changes** checkbox. This checkbox is enabled by default. If you leave the check box as is, the reference date will change when the system date changes.

   If you clear the checkbox, the reference date will continue to be the last date that was set by user, even if the system date changes.

4. To accept the changes, click **OK**.

   To exit the Edit Reference Date dialog box without changing the reference date, click **Cancel**.

5. To display the report with the date change, you must open another instance of the report.

How Do I Adjust the Reporting Timeframe?

The reporting time frame for each report is displayed as a part of the report's title. You can change the current report's time frame at any time by clicking on the **Change ReportÕs Timeframe** icon on the toolbar. The Change Report's Timeframe dialog box appears.

Each report is designed to run using a default time frame. The default time frame is based on the information provided in the report, for example, all *Management* and *End User* reports provide details for the last 28 day period starting with the previous day's date, while *Administrative* reports provide details for the previous day.

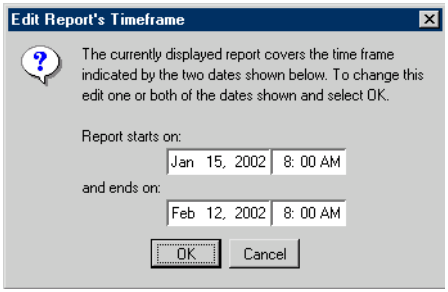
Advanced Reporter allows users to change the time frame used to run any of the reports. If you enter a start date/time that is greater than the end date/time, NBAR will swap them for you and display information for the period between the dates.

▼ To change the reportÕs time frame:

1. Click the **Change ReportÕs Timeframe** button on the toolbar, or, from the **Edit** menu, choose **Timeframe**.

   The Edit Report's Timeframe dialog box appears.

Edit Report Timeframe Dialog



2. Select new date(s) for the report. You can change the start date, the end date, or both. For each date, you can change the month, the day, the year, or the hour. If you only want to look at one day's worth of data, enter the same date in both fields.

3. Click **OK** to accept the selected dates, or **Cancel** to keep the time frame as is.

Advanced Reporter regenerates the currently displayed report using the newly selected time frame. If you have accessed the current report by following a link from another report, only the current report is generated using the new dates. To reload the higher level report using the new dates, click the **Previous Report** button on the toolbar, or select **Previous** from the **View** menu and repeat steps 1 to 3.

If you change the time frame of a report that has a Selection Criteria bar, the report subtitle will change, but the report will not be regenerated to reflect the new dates until you click the **Run** button again. This is designed to allow you to change the criteria for the report after choosing the timeframe.

What Determines the Timeframe for a Report?

Each report is defined with a default reporting period, or time frame. For some reports, the default time frame is 24 hours, or one day, and for others it is 28 or 30 days. Unless you specify a different starting date (by adjusting the Reference date), the report uses the day you run the report, as the last day of the reporting period. For example, assume you are running reports today. For reports with a one day time frame, today is both the first and

last day of the reporting period. For reports with a 30 day time frame, today is the last day of the reporting period, and 30 days prior to today is the first day. If today is June 22, a 30 day reporting period would run from May 24 - to June 22.

Advanced Reporter pulls the report data from NetBackup logs. Therefore, the time frame for each report is also based on NetBackup's time frames and that a 24-hour chunk of time is considered a 'day', though doesn't necessarily start at midnight. See "How NBAR defines a day," , for more information.

Some NBAR reports compare data from a current period with the same period a year ago. If NBAR does not have access to the data from a year ago (there is no data for that period in the NetBackup database), NBAR will use the oldest data available to calculate the annual percentage change. However, the calculations for percentage change will use the given timeframe, whether or not there is data available. This may result in empty entries. Choose your dates carefully when you are comparing trends in system activity across time.

How Does NBAR Count Backup Jobs?

Advanced Reporter understands the structure of NetBackup policies and records backup jobs' dates accordingly. When a Backup Window opens (typically backups are run overnight during the week and during the day on weekends), all backup jobs that are performed within that open window (regardless of the date they begin or finish) are recorded to have started on the date the Backup Window opened. For example, if a Backup Window opens at 8 p.m. on April 24th and closes at 6 a.m. on April 25th, all jobs (even those that started at 2 a.m. on April 25th) that ran in this window are dated April 24th. For more details on NetBackup Policies, Schedules and Backup Windows, refer to *NetBackup System Administrator's Guide.*

Each morning, at a time designated by the administrator, NBAR scans the NetBackup logs and extracts specific information to the NBAR database. NBAR follows the same reporting time frame principles as NetBackup. Backup jobs that ran under a Backup Window that opened on a Wednesday are reported under Wednesday's date even if the job started and finished on Thursday.

NBAR does not record backup information for jobs that were started but not finished when the NetBackup logs are scanned. This backup information will be recorded during the next scan by NBAR (assuming the backup job has been completed).

Restore jobs are reported in NBAR on the actual day they were performed.

How Do I Print the Selected Report?

You can print any of the generated reports.

- Click on the **Print the report** button on the toolbar or, from the **File** menu, select **Print** to print the currently displayed report.

Note If you are having trouble with reports that print without graphics, or are not complete, make sure that you have the latest drivers downloaded from the printer vendor.

How Do I Copy the Selected Report?

You can save any of the generated reports.

- Click on the **Copy** button on the toolbar or, from the **Edit** menu, select **Copy** to save the currently displayed report to the clipboard. You can then transfer the report's data to another format, such as a spreadsheet.

Starting the Java Applet GUI for the First Time

When you start Advanced Reporter for the first time, the application will install itself as an extension to your browser and run as a Java plug-in. The first thing that you will see will be a security message from your browser indicating that a request is being made to install a plug-in onto your workstation. Click **Yes** to accept the installation. If you are using Microsoft Internet Explorer, Advanced Reporter starts at this point. If you use Netscape Navigator, you must exit the browser completely and restart it before you can access Advanced Reporter.

Note If a new version of the plug-in is detected, it will automatically install on your web browser. Selecting the optional **Remember This Decision** checkbox will prevent the security messages from displaying during subsequent updates. If you want to remove the Java applet, please refer to your browser's documentation for information on how to remove a plug-in.

Starting the Java Applet GUI

We assume that any user running Advanced Reporter is familiar with the Internet and using a web browser. For information on the Netscape Navigator or Microsoft Internet Explorer web browsers, refer to the user documentation that came with the browser's software.

▼ There are two ways to start VERITAS NetBackup Advanced Reporter 4.5:

1. Start the web browser on your computer.

   a. Access the Advanced Reporter program by entering the Uniform Resource Locator (URL) in the **Location** or **Address** box and pressing [Return]. For example,

`http://servername.yourdomain:8885/nbar.html` `(Solaris or HP-UX)`
`http://servername.yourdomain/nbar/nbar.html` `(Windows NT/2000)`

Note This will not work if the NetBackup Administrator changed the http: server port during installation. Please contact your NetBackup Administrator to verify the URL if you are having trouble connecting to VERITAS NetBackup Advanced Reporter 4.5.

We suggest you add the Advanced Reporter program URL as a **Bookmark** or **Favorite** for easy access.

2. From the **Start** menu, choose **VERITAS NetBackup => Advanced Reporter => NetBackup Advanced Reporter**.

As Advanced Reporter is being loaded, the Loading NBAR window appears to show how much of NBAR has loaded. The **Start** button will appear on the opening screen after the application has loaded.

Viewing the Management Reports 4

This chapter provides details on each of the Management reports available with VERITAS NetBackup Advanced Reporter 4.5 (NBAR).

Overview of the NBAR Management Reports

The Management reports generated by NBAR provide summary information about an organization's VERITAS NetBackup backup (full and incremental) activities, restore activities, catalog usage, and operating errors.

Note User Backup jobs and Archive jobs are not included in the management reports, although they are shown by the NetBackup Activity Monitor.

These reports allow the manager to determine whether service commitments are being met, if the existing infrastructure is meeting the backup needs of their organization, and if the disk space allocated for the VERITAS NetBackup catalogs is sufficient.

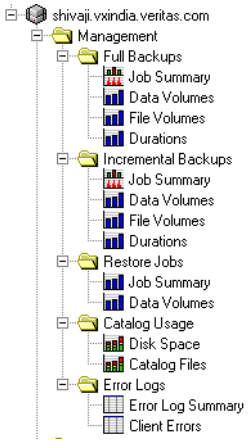
Each Management report consolidates the backup information from the last 28 day period starting with the previous day.

All Management reports appear under one of the following categories:

- Full Backups,
- Incremental Backups,
- Restore Jobs,
- Catalog Usage, or
- Error Logs.

The following window shows the **Management Reports** folder open, listing all available Management reports. Details on each Management report can be found in this chapter.

Management Reports Tree



Viewing the Full Backups Reports

The **Full Backups** folder contains four Management reports for all full backup jobs performed in the last 28 day period.

- *Job Summary (“Full Job Completion Summary Report.”)*
- *Data Volumes (“Full Backup Data Volumes Report.”*
- *File Volumes (“Full Backup File Volumes Report.”)*
- *Durations (“Full Backup Job Durations Report.”)*

Full Job Completion Summary Report

This report provides an overview of the full backup jobs for each day within the reporting period. The report displays two charts. The upper chart displays completely successful, partially successful, and failed jobs for each day. The lower chart displays the percent of jobs that failed for each backup.

This report allows you to quickly identify patterns and problem areas in your full backup activities. By default the reporting period is 28 days.

How to Access this Report

Select the **Job Summary** option from the **Full Backups** folder.

Report Details

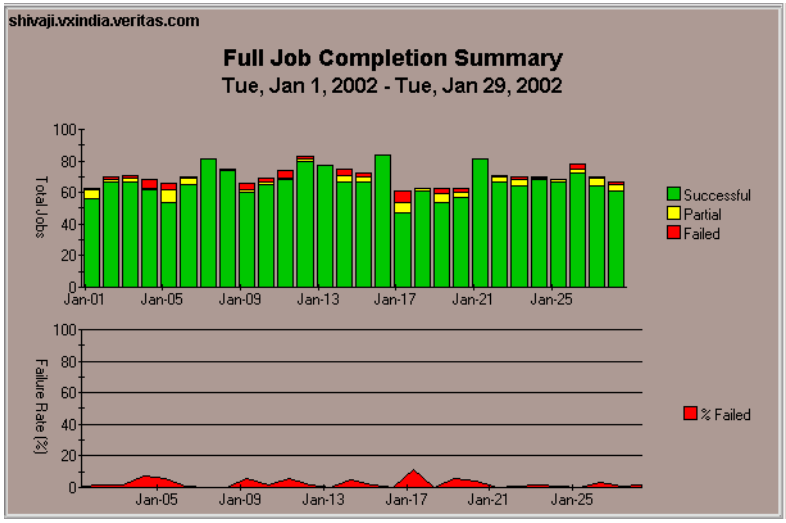
Each bar in the upper chart represents the number of full backup jobs for that date. The number of successful full backup jobs appears in green, yellow indicates the number of full backup jobs that were partially successful, and failed full backup jobs appear in red.

If you allow the cursor to hover over the bar for a particular day, a summary of the number of completely successful, partially successful, and failed jobs for that date appears in a popup window next to the cursor.

Click on a bar to display the *Backup Details by Policy - Full Backups* report for the day selected. Details include the number of bytes backed up, and an error summary for each failed job. For more information, see the *Backup Details by Policy Report*. Both of these reports display one entry for each job IDs. If a job had two retries, it will still only show up as one entry, as long as it was retried with the same job ID.

The lower chart displays the failure rate for each day's backup. Click on a bar to display the *Consolidated Error Log* for that day. For more information, see the *Consolidated Error Log*.

Full Job Completion Summary Report



Full Backup Data Volumes Report

This report provides an overview of the total volume of data that were backed up for each day within the reporting period. By default, the reporting period is 28 days. This report allows you to look for trends in the amount of data being backed up.

How to Access this Report

Select the **Data Volumes** option from the **Full Backups** folder.

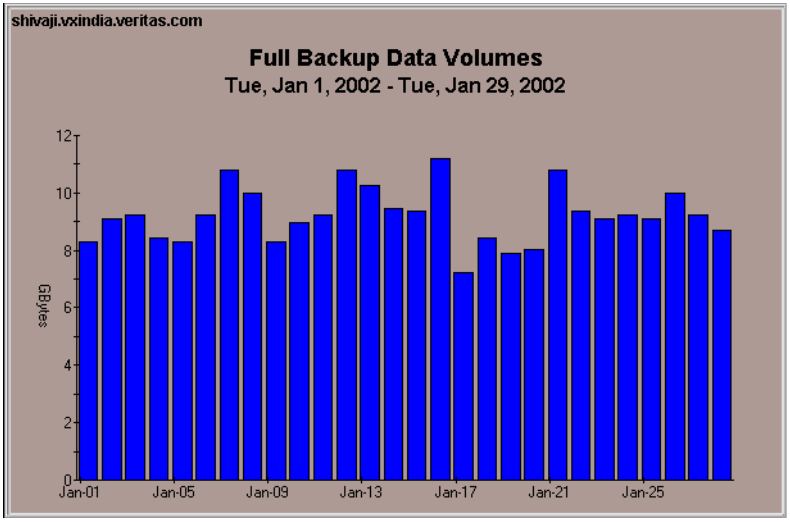
Report Details

Each bar represents the amount of data backed up for one day within the reporting period.

If you allow the cursor to hover over the bar for a particular day, a summary showing the amount of data backed up for that day appears in a popup window next to the cursor.

Each bar within this report is linked to a more detailed report for that day. When you click on a bar, the *Backup Details by Policy* report appears displaying more information for the day selected. For more information, see the *Backup Details by Policy Report*.

Full Backup Data Volumes Report



Full Backup File Volumes Report

This report provides a visual display of the total number of files that were backed up for each day within the reporting period. The default reporting period is the 28 days up to and including today's date.

How to Access this Report

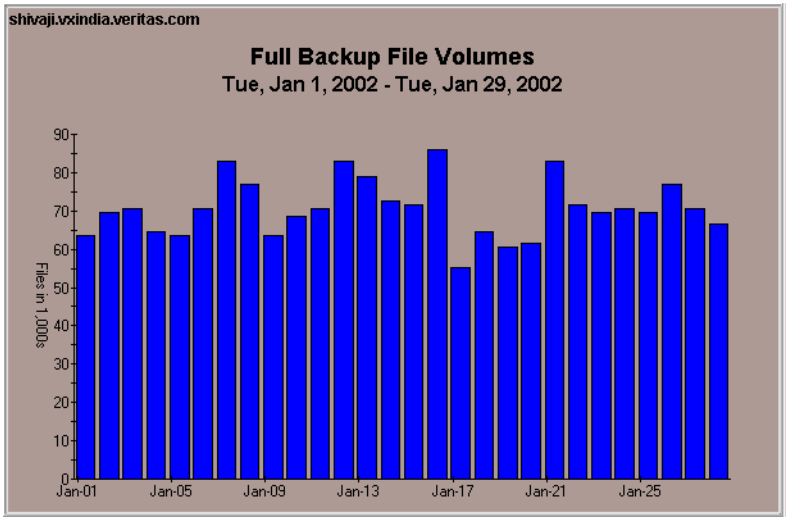
Select the **File Volumes** option from the **Full Backups** folder.

Report Details

Each bar in this report provides details on the total number of files grouped in 1,000's that were backed up for each date within the reporting period.

If you allow the cursor to hover over a bar, the number of files backed up for that date will appear in a popup window next to cursor. When you click on any bar, the *Backup Details by Policy* report appears displaying detailed information for the day selected. For more information, see the "Backup Details by Policy Report" on page 104.

Full Backup File Volumes Report



Full Backup Job Durations Report

This report provides a visual display of the total amount of time per day that was committed to full backup for each day within the reporting period.

It provides an indication of the number of hours per day NetBackup had an active policy.

How to Access this Report

Select the **Durations** option from the **Full Backups** folder.

Report Details

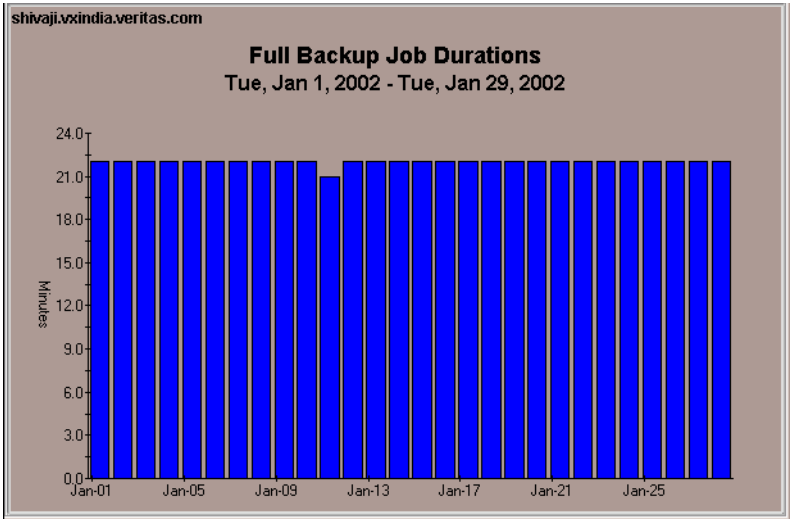
Each bar in this report provides details on the total amount of time in hours during which full backup jobs were active each day within the reporting period.

Note Job duration totals are calculated based on the total time the policy was active, that is, from the start of the first job within the reporting period to the end of the last job within the reporting period. For example, if the first job begins 01/01/2001 at 10 a.m. and lasts for 5 minutes, and the last job begins 01/01/2001 at 11 a.m. and lasts 5 minutes, the total job duration reported will be from 10 a.m. to 11:05 a.m., a total of 1 hours and 5 minutes, even though the actual backup time totaled 10 minutes.

If you allow the cursor to hover over the bar for a particular date, the date and the number of hours and minutes a policy was active appears in a popup window next to the cursor.

Clicking on any bar displays the *Backup Details by Policy* report for that day. For more information, see the "Backup Details by Policy Report" on page 104.

Full Backup Job Durations Report



Viewing the Incremental Backups Reports

The **Incremental Backups** folder contains four *Management* reports for all incremental backup jobs performed in the last 28 day period.

- *Job Summary (“Incremental Job Completion Summary Report.”)*
- *Data Volumes (“Incremental Backup Data Volumes Report.”)*
- *File Volumes (“Incremental Backup File Volumes Report.”*
- *Durations (“Incremental Backup Job Durations Report.”)*

Incremental Job Completion Summary Report

This report provides an overview of the incremental backup jobs for each day within the reporting period. This report includes both cumulative-incremental backups and differential-incremental backups. It differentiates between completely successful, partially successful, and failed jobs. You can quickly identify problem areas and patterns in your incremental backups.

How to Access this Report

Choose **Job Summary** from the **Incremental Backups** folder.

Report Details

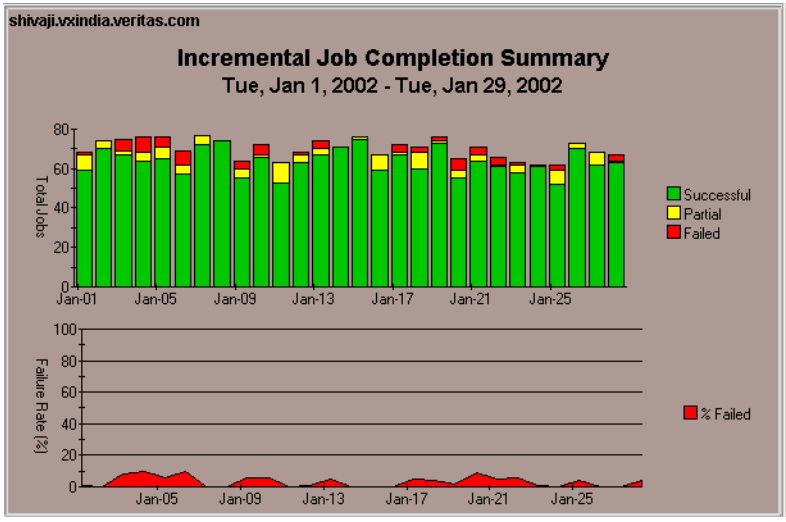
Each bar in the upper chart represents the number of incremental backup jobs for that date. The number of successful incremental backup jobs appears in green, yellow indicates the number of incremental backup jobs that were partially successful, and failed incremental backup jobs appear in red.

If you allow the cursor to hover over the bar for a particular day, a summary of the number of completely successful, partially successful, and failed jobs for that date appears in a popup window next to the cursor.

Click on a bar to display the *Backup Details by Policy - Incremental Backups* report for the day selected. Details include the number of bytes backed up, and an error summary for each failed job. For more information, see the *Backup Details by Policy Report*.

The lower chart displays the failure rate for each day's backups. Click on a bar to display the *Consolidated Error Log* for that day. For more information, see the *"Consolidated Error Log" on page 106*.

Incremental Job Completion Summary Report



Incremental Backup Data Volumes Report

This report provides an overview of the total amount of data that was backed up during incremental backup jobs for each day within the reporting period. You can quickly identify trends in the amount of data backed up in incremental backup jobs each day.

How to Access this Report

Choose **Data Volumes** from the **Incremental Backups** folder.

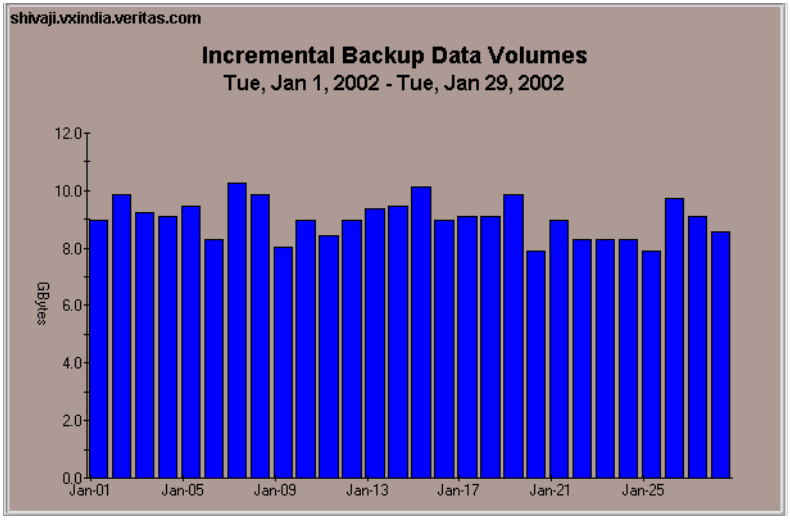
Report Details

Each bar represents the amount of data backed up for one day within the reporting period.

If you allow the cursor to hover over the bar for a particular day, a summary showing the amount of data backed up for that day appears in a popup window next to the cursor.

Each bar within this report is linked to a more detailed report for that day. When you click on a bar, the *Backup Details by Policy - Incremental Backups* report appears displaying more information for the day selected. See the "Backup Details by Policy Report" on page 104.

Incremental Backup Data Volumes Report



Incremental Backup File Volumes Report

This report provides a visual display of the total number of files that were backed up for each day within the reporting period for all incremental backups. You can quickly identify trends in the number of files backed up.

How to Access this Report

Choose **File Volumes** from the **Incremental Backups** folder.

Report Details

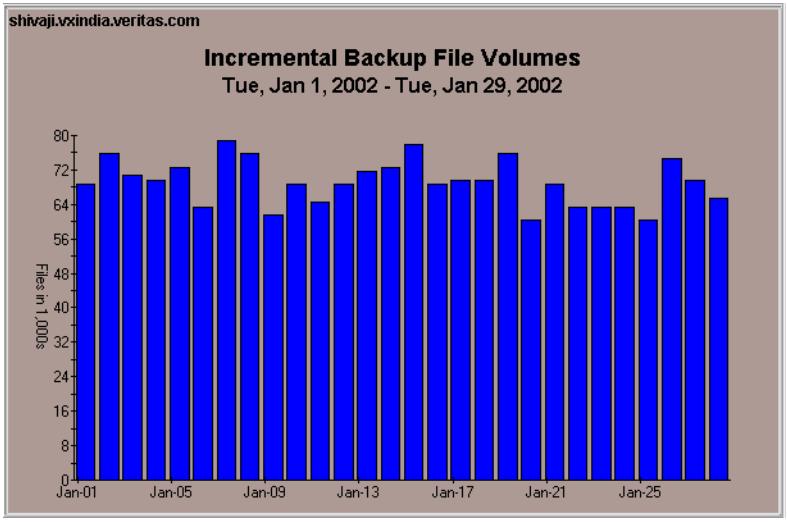
Each bar in this report provides details on the total number of files, grouped in 1,000's, that were backed up for each day within the reporting period for all incremental backups.

If you use the cursor to hover over a bar, the total number of files backed up will display.

If you right-click on a bar, the context-sensitive menu displays.

Each bar within this report represents one day in the time period selected. Clicking on any bar links to the *Backup Details by Policy* report displaying Incremental Data information for that day. See the "Backup Details by Policy Report" on page 104.

Incremental Backup File Volumes Report



Incremental Backup Job Durations Report

This report provides a visual display of the total amount of time in each day that was committed to incremental backup.

You can quickly estimate how many hours per day NetBackup had an active policy.

How to Access this Report

Choose **Durations** from the **Incremental Backups** folder.

Report details

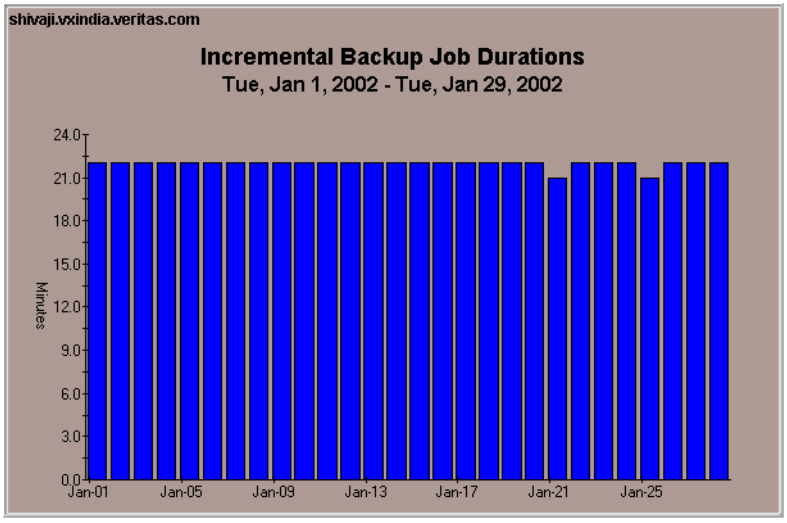
Each bar in this report provides details on the total amount of time during which incremental backup job policies were active each day within the reporting period.

If you allow the cursor to hover over the bar for a particular date, the date and the number of hours and minutes a policy was active appears in a popup window next to the cursor.

Each bar within this report represents one day in the time period selected. Clicking on any bar links to the *Backup Details by Policy - Incremental Backups* report. For more information, see the "Backup Details by Policy Report" on page 104.

Note Job duration totals are calculated based on the total time the policy was active, that is, from the start of the first job within the reporting period, to the end of the last job within the reporting period. For example, if the first job begins 01/01/2000 at 10 a.m. and lasts for 5 minutes, and the last job begins 01/01/2000 at 11 a.m. and lasts 5 minutes, the total job duration reported will be from 10 a.m. to 11:05 a.m., a total of 1 hours and 5 minutes, even though the actual backup time totaled 10 minutes.

Incremental Backup Job Durations Report



Viewing the Restore Jobs Reports

The **Restore Jobs** folder contains two *Management* reports that provide details on the restore jobs performed in the last 28 day period.

- *Job Summary (“Restore Job Summary Report.”)*
- *Data Volumes (“Restore Data Volumes Report.”)*

Restore Job Summary Report

This report provides an overview of all the jobs that were restored to a client machine within the time period selected. The default reporting period is the 28 days preceding today's date.

You can quickly determine how often restore jobs are being performed and calculate their rate of success.

How to Access this Report

This report is generated by:

- Choosing **Job Summary** from the **Restore Jobs** folder.
- Clicking on the **Restore Jobs** section sub-title in the *Site Summary* report (data displayed is for all restore jobs performed on the date on the *Site Summary* report).

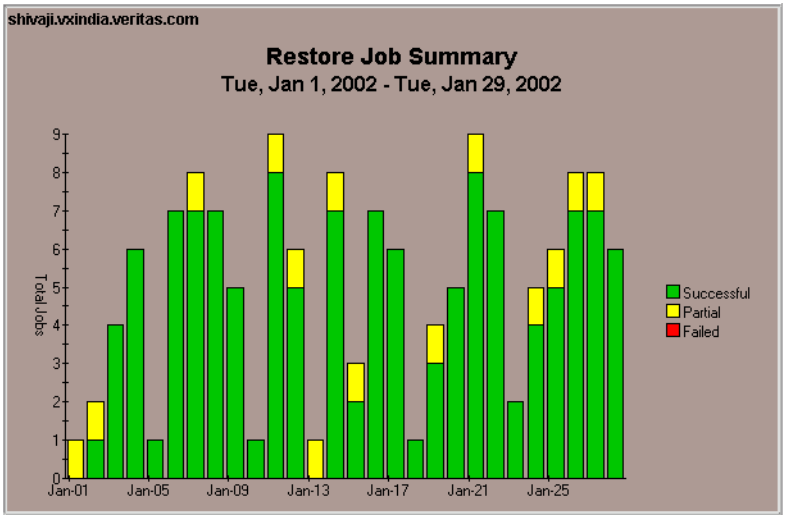
Report Details

Each bar in this report provides details on the total number of restore jobs for each day in the reporting period. The number of successful restore jobs appears in green, yellow indicates the number of restore jobs that were partially successful, and failed restore jobs appear in red.

If you allow the cursor to hover over the bar for a particular day, the number of completely successful, partially successful, and failed jobs for that date appears in a popup window next to the cursor.

Click on any bar to link to the *Restore Details by Client* report displaying the amount of information restored for the day selected. For more information, see the "Restore Details by Client Report" on page 109.

Restore Job Summary Report



Restore Data Volumes Report

This report provides an overview of all the data volumes that were restored for each day within the reporting period.

You can quickly identify trends in the amount of data restored.

How to Access this Report

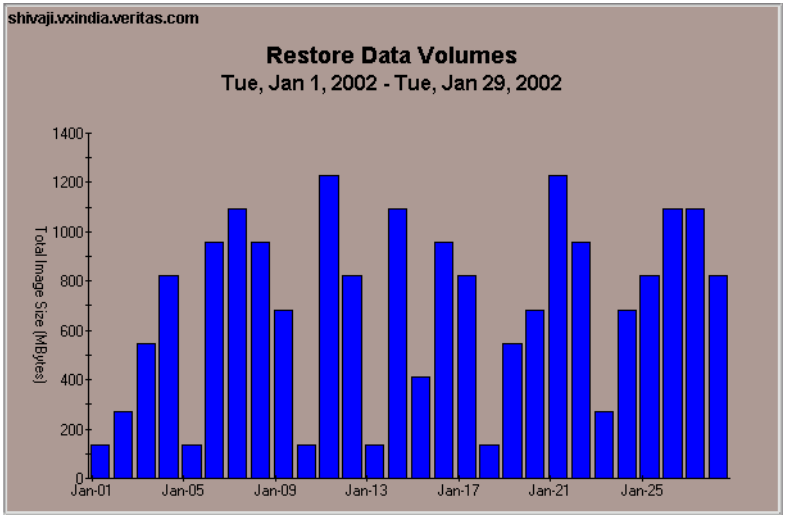
Choose **Data Volumes** from the **Restore Jobs** folder.

Report Details

Each bar in this report provides details on the total size of all images read to complete the restore jobs for that day) within the reporting period.

Each bar within this report represents one day in the time period selected. Click on any bar to link to the *Restore Details by Client* report to display information on the data restored for the day selected. For more information, see the “Restore Details by Client Report” on page 109.

Restore Data Volumes Report



Viewing the Catalog Usage Reports

The **Catalog Usage** folder contains two *Management* reports:

- *Disk Space* (“Disk Space Report,”) and
- *Catalog Files* (“Number of Catalog Files Report”).

Each of these reports provides details on the VERITAS NetBackup Master server’s catalog for the last 28 day period. Each catalog is a log containing the information on every backup job that has not yet expired. (When backup jobs expire, VERITAS NetBackup automatically removes the backup job from the catalog.) It is important that the servers do not run out of the disk space allotted to these catalogs. These reports allow you to monitor how much disk space is currently being used so you can determine how much is still available.

Disk Space Report

This report displays the total amount of disk space currently in use by the VERITAS NetBackup servers' catalog files.

You can conveniently keep track of the amount of disk space being used by the catalog files, and you will have a chance to increase disk space before the catalog files exceed the currently allotted amount of space.

How to Access this Report

Choose **Disk Space** from the **Catalog Usage** folder.

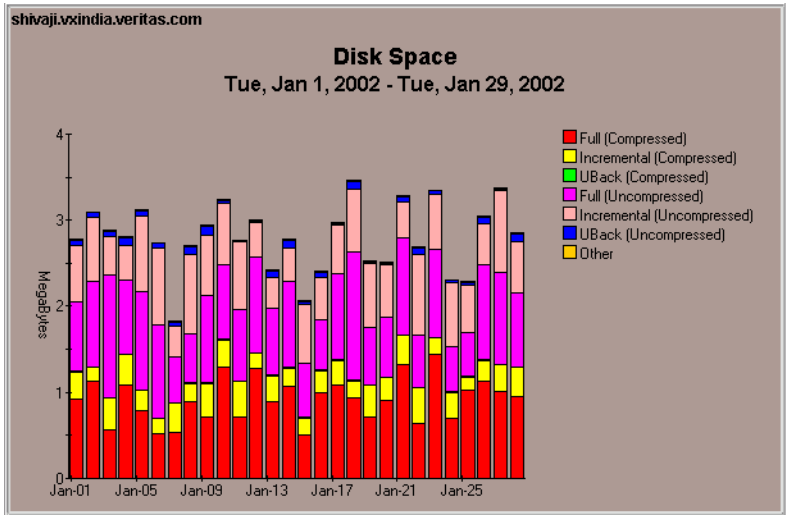
Report Details

Each bar in this report provides details on the total disk space being used (vertical axis) for each day (horizontal axis) within the reporting period. The bar is divided into colors based on the type of backup data reflected.

- Full backup data that is compressed is shown in red;
- Incremental backup data that is compressed is shown in yellow;
- User Directed backup data that is compressed is shown in green;
- Full backup data that is uncompressed appears in hot pink;
- Incremental backup data that is uncompressed is shown in light pink;
- User Directed backup data that is uncompressed is shown in blue;
- Other disk utilization, such as File System Overheads, is shown in gold.

If you allow the cursor to hover over the bar for a particular day, a summary of the amount of each type of data stored on the disk for that day is displayed.

Disk Space Report



Number of Catalog Files Report

This report displays the total number of catalog (.f) files that are currently in the catalog on the NetBackup master servers.

How to Access this Report

The *Number of Catalog Files* report is generated by selecting the **Catalog Files** option from the **Catalog Usage** folder.

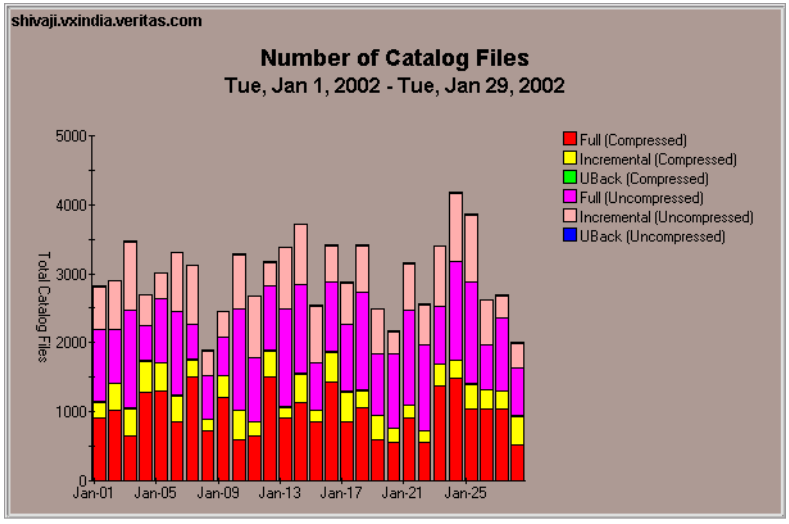
Report Details

Each bar in this report provides details on the total number of catalog files (vertical axis) backed up for each day (horizontal axis) within the reporting period.

- Full backup files that are compressed are shown in red;
- Incremental backup files that are compressed are shown in yellow;
- User Directed backup files that are compressed are shown in green;
- Full backup files that are uncompressed are shown in hot pink;
- Incremental backup files that are uncompressed are shown in light pink;
- User Directed backup files that are uncompressed are shown in blue.

If you allow the cursor to hover over the bar for a particular day, a summary of the number of catalog files of each type of data stored on the disk for that day is displayed.

Number of Catalog Files Report



Viewing the Error Logs

The **Error Logs** folder contains two *Management* reports Each of these reports provide a summary of the VERITAS NetBackup's Error Log catalog for the last 28 day period.

- *Error Log Summary ("Error Log Summary Report")*
- *Client Error ("Error Log Summary by Client Report")*

Error Log Summary Report

This report displays a list of all the VERITAS NetBackup errors that occurred in the reporting period by server.

You can easily identify patterns, trouble areas, and common problems with your backup activities.

How to Access this Report

Choose **Error Log Summary** from the **Error Logs** folder.

Report Details

This report lists how many times an error has occurred on a server, and provides a brief description of the error.

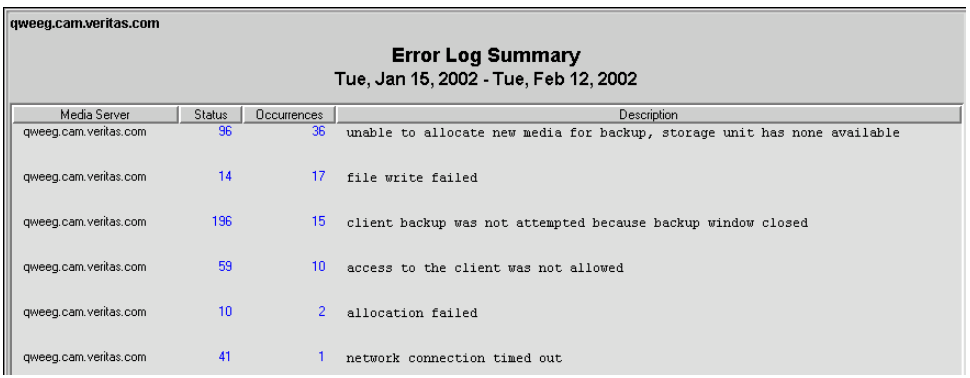
Click on the label for any field to sort entries by that field.

This report totals the number of errors, including retries. For example, if you had five job IDs that each had two retries, and all produced the error 57, the report would represent this as one entry for error code 57 with 10 occurrences.

All entries in the **Status** and **Occurrences** fields of this report link to more detailed reports.

- Click any entry in the **Status** field to access the *NetBackup Trouble Shooting Guide*. See the "NetBackup Trouble Shooting Guide" on page 140.
- Click any entry in the **Occurrences** field to access the *Summary of Status Code (number)* report. For more information, see the "Summary of Status Code <number> Report" on page 137.

Error Log Summary Report



qweeg.cam.veritas.com

Error Log Summary

Tue, Jan 15, 2002 - Tue, Feb 12, 2002

Media Server	Status	Occurrences	Description
qweeg.cam.veritas.com	96	36	unable to allocate new media for backup, storage unit has none available
qweeg.cam.veritas.com	14	17	file write failed
qweeg.cam.veritas.com	196	15	client backup was not attempted because backup window closed
qweeg.cam.veritas.com	59	10	access to the client was not allowed
qweeg.cam.veritas.com	10	2	allocation failed
qweeg.cam.veritas.com	41	1	network connection timed out

Error Log Summary by Client Report

This report displays a list of all the VERITAS NetBackup errors organized by client. You can easily identify patterns, trouble areas, and common problems with your backup activities.

How to Access this Report

Choose **Error Log Summary by Client** from the **Error Logs** folder.

Report Details

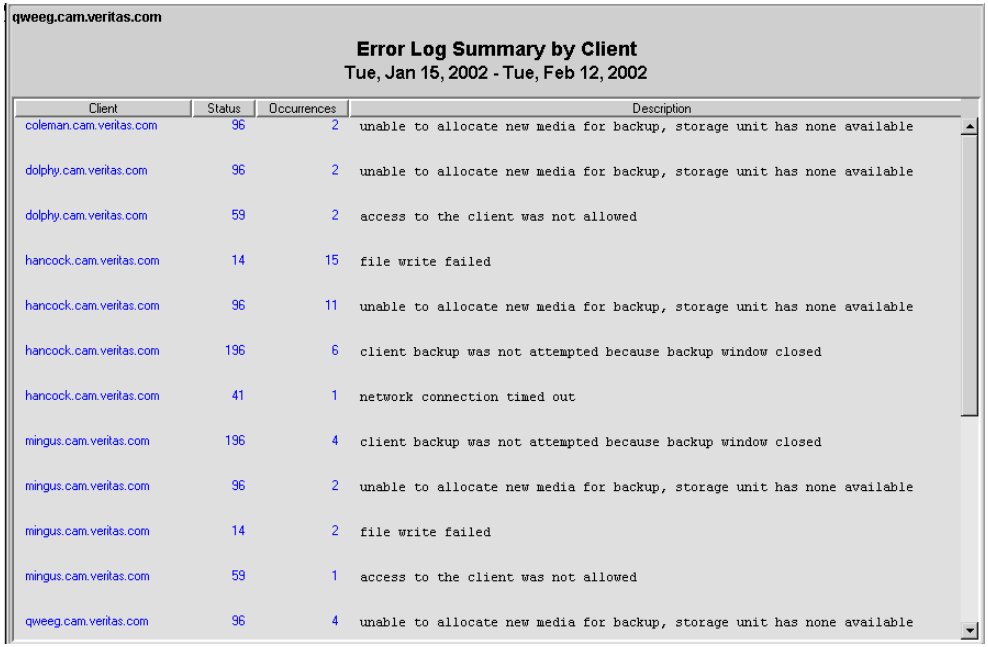
Click on the label for any field to sort entries by that field.

This report summarizes each client by job ID. If five jobs ran on five clients, and each job had two retries that ended in error 57, the report will show two retries for each client, and five entries with a status 57.

All entries in the **Client, Status** and **Occurrences** fields link to more detailed reports.

- Click any entry in the **Client** field to access the *Summary of Status Code for (Client)* report. For more information, see the "Summary of Status Codes for <client> Report" on page 138.
- Click any entry in the **Status** field to access the *NetBackup Trouble Shooting Guide*. See the "NetBackup Trouble Shooting Guide" on page 140.
- Click any entry in the **Occurrences** field to access the *Summary of Status Code (number) for (Client)* report. For more information, see the "Summary of Status Code <number> for <client> Report" on page 139.

Error Log Summary by Client Report



qweeg.cam.veritas.com

Error Log Summary by Client

Tue, Jan 15, 2002 - Tue, Feb 12, 2002

Client	Status	Occurrences	Description
coleman.cam.veritas.com	96	2	unable to allocate new media for backup, storage unit has none available
dolphy.cam.veritas.com	96	2	unable to allocate new media for backup, storage unit has none available
dolphy.cam.veritas.com	59	2	access to the client was not allowed
hancock.cam.veritas.com	14	15	file write failed
hancock.cam.veritas.com	96	11	unable to allocate new media for backup, storage unit has none available
hancock.cam.veritas.com	196	6	client backup was not attempted because backup window closed
hancock.cam.veritas.com	41	1	network connection timed out
mingus.cam.veritas.com	196	4	client backup was not attempted because backup window closed
mingus.cam.veritas.com	96	2	unable to allocate new media for backup, storage unit has none available
mingus.cam.veritas.com	14	2	file write failed
mingus.cam.veritas.com	59	1	access to the client was not allowed
qweeg.cam.veritas.com	96	4	unable to allocate new media for backup, storage unit has none available

Viewing the Administrative Reports 5

This chapter provides details on each of the Administrative reports available with VERITAS NetBackup Advanced Reporter 4.5 (NBAR).

Overview of NBAR Administrative Reports

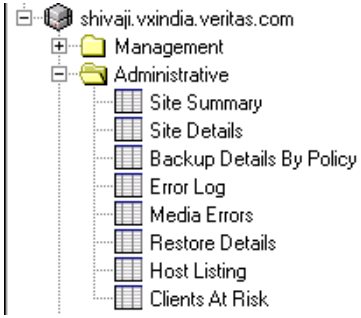
The Administrative reports generated by NBAR provide detailed information about an organization's storage resources. This information details whether daily backups are being performed successfully, and if not, where the problems are; and are devices operating correctly with no undetected problems. These reports allow the Administrative staff to quickly review NetBackup activities without resorting to culling information from the lengthy NetBackup Error Logs, thus allowing the Administrators to be more effective and responsive to their user's needs.

Each Administrative report consolidates the backup information from the previous day. The Administrative reports include:

- *Site Summary ("Site Summary Report"),*
- *Site Details ("Site Details Job List"),*
- *Backup Details by Policy ("Backup Details by Policy Report"),*
- *Error Log ("Consolidated Error Log"),*
- *Media Errors ("Media Errors Report"),*
- *Restore Details ("Restore Details by Client Report"),*
- *Host Listing ("Hosts under NetBackup Management Report"),*
- *Clients at Risk ("Clients at Risk Report")*

The following console tree displays all available Administrative reports. Details on each Administrative report can be found in this chapter.

Tree menu displaying Administrative reports



Site Summary Report

The *Site Summary* report presents summaries of four types of NetBackup activity: full and incremental backup jobs, restore jobs, error log data, and a summary of the health of the backup system for a particular 24 hours. The *Site Summary* report allows you to quickly identify problem areas or patterns in the displayed day's backup.

How to Access this Report

- Select the **Site Summary** option from the **Administrative** folder in the Report Generator window (data is displayed for all backup jobs - full and incremental - performed on the previous day), or
- Double-click on any bar in the *Full Job Completion Summary* report or the *Incremental Job Completion Summary* report in the **Management** folder (data displayed is for all backup jobs - full and incremental - performed on the specific day selected).

Report Details

Note The number of failed jobs recorded under the Backup Jobs summary may not be the same as the number in the Error Log Summary. This is because the Backup Jobs report only records unsuccessful jobs, while the Error Log Summary records every unsuccessful attempt. Therefore, if a job is attempted twice and fails twice, there will be one entry under Backup Jobs, and two under the Error Log Summary.

The *Site Summary* report provides information on:

- Backup Jobs - summary statistics on the total number of jobs backed up in the 24 hours before the totals for this report were calculated. The data in this section consists of: total successful, partial and failed jobs; total amount of data; total number of files; and the total elapsed time in hours, minutes and seconds for all jobs.

  Click the Backup Jobs section sub-title to access the *Backup Details by Policy* report. For more information, see the "Backup Details by Policy Report" on page 104.

- Restore Job Summary- details on the number of restore jobs requested and failed in the 24 hours before the totals for this report were calculated; average time in seconds for a restore job; number of jobs that exceeded one hour; total amount of data restored; and the average amount of data restored per job.

  Click the Restore Jobs section sub-title to access the *Restore Job Summary* report. See "Restore Job Summary Report" on page 87.

- Error Log Summary – gives a detailed summary of the NetBackup Error Log for the 24 hours before totals for this report were calculated. The error types include: Connection Failures; Backup Window Closed; Hit Skipped File Limit; Skipped or aborted jobs; and other errors.

  Click on the Error Log Summary section sub-title to access the *Error Log Summary* report. For more information, see the "Error Log Summary Report" on page 96.

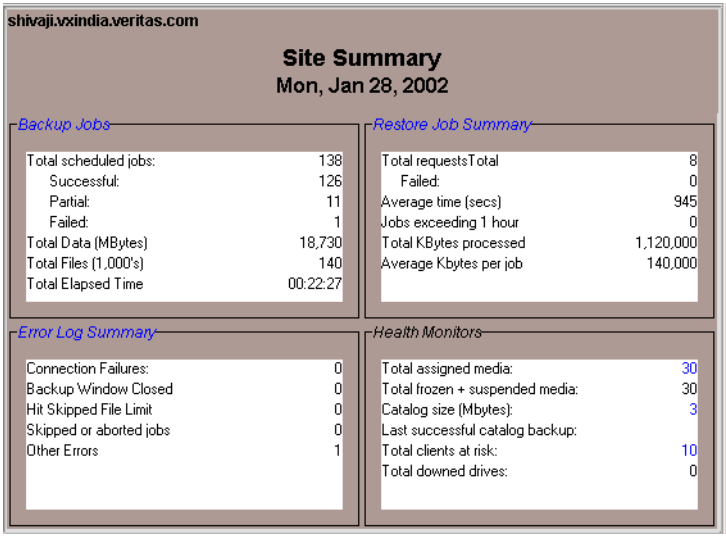
- Health Monitors– The data in this section covers media status, catalog size and last successful backup, clients at risk, and downed drives. The data for these values reflects the state of the system the last time the loader ran.

  The Clients at Risk entry on the Health Monitor links to the *Clients at Risk* report. For more information, see "Clients at Risk Report" on page 111.

  The Catalog Size entry links to the Disk Space report. For more information, see "Disk Space Report" on page 91.

  The Total Active Media entry links to the Active Media List report. For more information, see "Assigned Media List" on page 115.

Site Summary Report



shivaji.vxindia.veritas.com

Site Summary
Mon, Jan 28, 2002

Backup Jobs

Total scheduled jobs:	138
Successful:	126
Partial:	11
Failed:	1
Total Data (MBytes)	18,730
Total Files (1,000's)	140
Total Elapsed Time	00:22:27

Restore Job Summary

Total requestsTotal	8
Failed:	0
Average time (secs)	945
Jobs exceeding 1 hour	0
Total KBytes processed	1,120,000
Average Kbytes per job	140,000

Error Log Summary

Connection Failures:	0
Backup Window Closed	0
Hit Skipped File Limit	0
Skipped or aborted jobs	0
Other Errors	1

Health Monitors

Total assigned media:	30
Total frozen + suspended media:	30
Catalog size (Mbytes):	3
Last successful catalog backup:	
Total clients at risk:	10
Total downed drives:	0

Site Details Job List

The *Site Details Job List* provides details on all of the jobs that ran in the last 24 hour period.

This report allows you to view summary information on each job, in chronological order, without regard for policy or schedule. All jobs, including those with errors, are displayed.

How to Access this Report

Select the **Site Details** option from the **Administrative** folder in the Report Generator window.

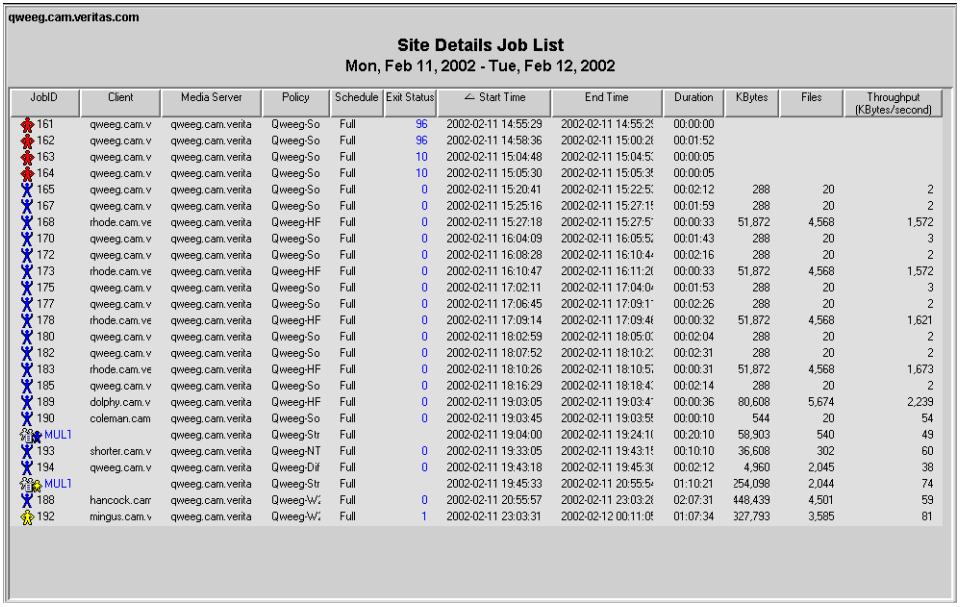
Report Details

By default, data is displayed for all backup jobs - full and incremental – scheduled for the previous day.

An entry in the **Exit Status** field may link to a more detailed report.

- Click on any entry in the **Exit Status** field to access the *NetBackup Trouble Shooting Guide*. For more information, see the "NetBackup Trouble Shooting Guide" on page 140.

Site Details Job List



qweeg.cam.veritas.com

Site Details Job List
Mon, Feb 11, 2002 - Tue, Feb 12, 2002

JobID	Client	Media Server	Policy	Schedule	Exit Status	Start Time	End Time	Duration	KBytes	Files	Throughput (KBytes/second)
161	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	96	2002-02-11 14:55:29	2002-02-11 14:55:2	00:00:00			
162	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	96	2002-02-11 14:58:36	2002-02-11 15:00:2	00:01:52			
163	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	10	2002-02-11 15:04:48	2002-02-11 15:04:5	00:00:05			
164	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	10	2002-02-11 15:05:30	2002-02-11 15:05:3	00:00:05			
165	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 15:20:41	2002-02-11 15:22:5	00:02:12	288	20	2
167	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 15:25:16	2002-02-11 15:27:1	00:01:59	288	20	2
168	rhode.cam.ve	qweeg.cam.verita	Qweeg-HF	Full	0	2002-02-11 15:27:18	2002-02-11 15:27:5	00:00:33	51,872	4,568	1,572
170	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 16:04:09	2002-02-11 16:05:5	00:01:43	288	20	3
172	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 16:08:28	2002-02-11 16:10:4	00:02:16	288	20	2
173	rhode.cam.ve	qweeg.cam.verita	Qweeg-HF	Full	0	2002-02-11 16:10:47	2002-02-11 16:11:2	00:00:33	51,872	4,568	1,572
175	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 17:02:11	2002-02-11 17:04:0	00:01:53	288	20	3
177	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 17:06:45	2002-02-11 17:09:1	00:02:26	288	20	2
178	rhode.cam.ve	qweeg.cam.verita	Qweeg-HF	Full	0	2002-02-11 17:09:14	2002-02-11 17:09:4	00:00:32	51,872	4,568	1,621
180	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 18:02:59	2002-02-11 18:05:0	00:02:04	288	20	2
182	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 18:07:52	2002-02-11 18:10:2	00:02:31	288	20	2
183	rhode.cam.ve	qweeg.cam.verita	Qweeg-HF	Full	0	2002-02-11 18:10:26	2002-02-11 18:10:5	00:00:31	51,872	4,568	1,673
185	qweeg.cam.v	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 18:16:29	2002-02-11 18:18:4	00:02:14	288	20	2
189	dolphy.cam.v	qweeg.cam.verita	Qweeg-HF	Full	0	2002-02-11 19:03:05	2002-02-11 19:03:4	00:00:36	80,608	5,674	2,239
190	coleman.cam	qweeg.cam.verita	Qweeg-So	Full	0	2002-02-11 19:03:45	2002-02-11 19:03:5	00:00:10	544	20	54
MUL1		qweeg.cam.verita	Qweeg-Str	Full		2002-02-11 19:04:00	2002-02-11 19:24:1	00:20:10	58,903	540	49
193	shorter.cam.v	qweeg.cam.verita	Qweeg-NT	Full	0	2002-02-11 19:33:05	2002-02-11 19:43:1	00:10:10	36,608	302	60
194	qweeg.cam.v	qweeg.cam.verita	Qweeg-Dif	Full	0	2002-02-11 19:43:18	2002-02-11 19:45:3	00:02:12	4,960	2,045	38
MUL1		qweeg.cam.verita	Qweeg-Str	Full		2002-02-11 19:45:33	2002-02-11 20:55:5	01:10:21	254,098	2,044	74
188	hancock.cam	qweeg.cam.verita	Qweeg-W2	Full	0	2002-02-11 20:55:57	2002-02-11 23:03:2	02:07:31	448,439	4,501	59
192	mingus.cam.v	qweeg.cam.verita	Qweeg-W2	Full	1	2002-02-11 23:03:31	2002-02-12 00:11:0	01:07:34	327,793	3,585	81

Backup Details by Policy Report

The *Backup Details by Policy* report provides details on the jobs scheduled to run for specific policies. The report allows you to view summary information on each policy that had a backup run the previous day.

How to Access this Report

There are three ways to access this report:

- Select the **Details by Policy** option from the **Administrative** folder in the NBAR Report Generator window. Data is displayed for all backup jobs, both full and incremental, performed on the previous day.
- Click on any bar in the *Full Data* report, *Full Files* report, *Incremental Data* report, or *Incremental Files* report. Data displayed is for full or incremental backup jobs performed on the specified 24 hour period.
- Click on the **Backup Jobs** Report Link sub-title in the *Site Summary* report. Data displayed is for the same date as the *Site Summary* report.

Report Details

NBAR considers the start time for the policy to be the beginning of the first *successful* job run for each policy. You may see job start times within each policy that are prior to the start time for the policy listed in the **Start Time** column of the report if the first jobs run were unsuccessful.

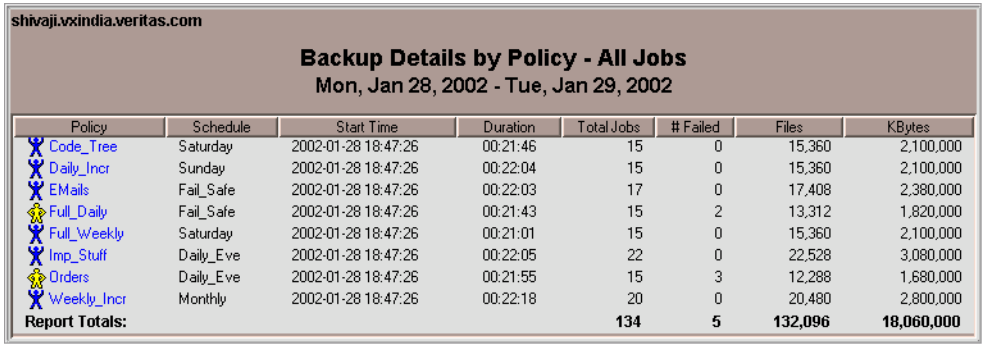
In addition, the **Total Jobs** field reflects the number of *successful* jobs --- it does not include the number of times NetBackup attempted unsuccessfully to run a job.

This report may show multiple entries for each policy name / schedule name pair if a change to the Netbackup policy definition occurs during the report's time frame. Jobs which were run with a policy definition that has become outdated will have the word 'retired' appended to the policy name.

Each entry in the **Policy** field links to a more detailed report.

- Click on any entry in the **Policy** field to access the *Job Details for NetBackup Policy (Policy name)* report. For more information, see the "Job Details for NetBackup Policy <policy name> Report" on page 142.

Backup Details by Policy Report



shivaji.vxindia.veritas.com

Backup Details by Policy - All Jobs

Mon, Jan 28, 2002 - Tue, Jan 29, 2002

Policy	Schedule	Start Time	Duration	Total Jobs	# Failed	Files	KBytes
Code_Tree	Saturday	2002-01-28 18:47:26	00:21:46	15	0	15,360	2,100,000
Daily_Incr	Sunday	2002-01-28 18:47:26	00:22:04	15	0	15,360	2,100,000
EMails	Fail_Safe	2002-01-28 18:47:26	00:22:03	17	0	17,408	2,380,000
Full_Daily	Fail_Safe	2002-01-28 18:47:26	00:21:43	15	2	13,312	1,820,000
Full_Weekly	Saturday	2002-01-28 18:47:26	00:21:01	15	0	15,360	2,100,000
Imp_Stuff	Daily_Eve	2002-01-28 18:47:26	00:22:05	22	0	22,528	3,080,000
Orders	Daily_Eve	2002-01-28 18:47:26	00:21:55	15	3	12,288	1,680,000
Weekly_Incr	Monthly	2002-01-28 18:47:26	00:22:18	20	0	20,480	2,800,000
Report Totals:				**134**	**5**	**132,096**	**18,060,000**

Consolidated Error Log

This report displays a consolidated list, by server and client, of all the errors that occurred during the previous day's backup. By default, all details that appear on this report are taken from the previous day's NetBackup Error Log.

This report allows you to review the error log and identify what errors occurred on which client.

How to Access this Report

- Click on the **Error Log** option in the **Administration** folder or
- Click on a point in the lower chart in the *Full Job Completion Summary* or *Incremental Job Completion Summary* reports.

Report Details

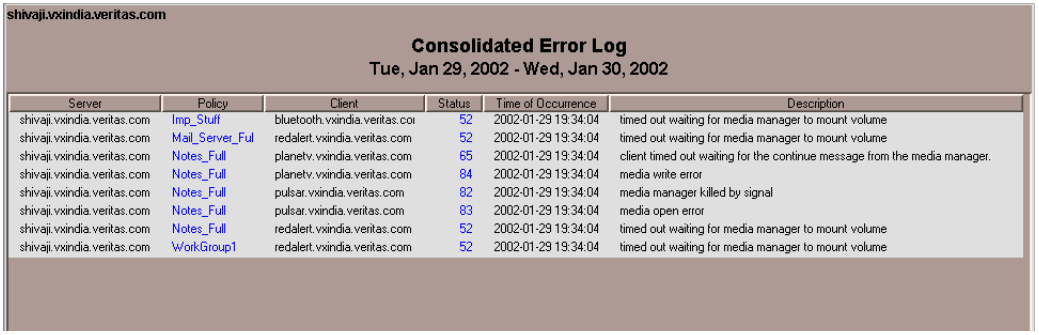
This report lists details for each server and its policy, including all clients on the server. Details for each client include the code for the error, the date and time the error occurred, and a description of the error. Clicking on the label for any field allows you to sort report entries by that field.

This report lists one entry for each occurrence of an error. If a job is retried with the same job ID, each retry will be listed on a separate line.

Each entry in the **Policy** and **Status** fields of this report are "Report Links" to more detailed reports.

- Click on any entry in the **Policy** field to access the *Job Details for NetBackup (Policy Name)* report. See the Job Details for NetBackup Policy <policy name> Report.
- Click on any entry in the **Status** field to access the *NetBackup Trouble Shooting Guide*. For more information see the "NetBackup Trouble Shooting Guide" on page 140.

Consolidated Error Log



shivaji.vxindia.veritas.com

Consolidated Error Log

Tue, Jan 29, 2002 - Wed, Jan 30, 2002

Server	Policy	Client	Status	Time of Occurrence	Description
shivaji.vxindia.veritas.com	Imp_Stuff	bluetooth.vxindia.veritas.co	52	2002-01-29 19:34:04	timed out waiting for media manager to mount volume
shivaji.vxindia.veritas.com	Mail_Server_Ful	redalert.vxindia.veritas.com	52	2002-01-29 19:34:04	timed out waiting for media manager to mount volume
shivaji.vxindia.veritas.com	Notes_Full	planetv.vxindia.veritas.com	65	2002-01-29 19:34:04	client timed out waiting for the continue message from the media manager.
shivaji.vxindia.veritas.com	Notes_Full	planetv.vxindia.veritas.com	84	2002-01-29 19:34:04	media write error
shivaji.vxindia.veritas.com	Notes_Full	pulsar.vxindia.veritas.com	82	2002-01-29 19:34:04	media manager killed by signal
shivaji.vxindia.veritas.com	Notes_Full	pulsar.vxindia.veritas.com	83	2002-01-29 19:34:04	media open error
shivaji.vxindia.veritas.com	Notes_Full	redalert.vxindia.veritas.com	52	2002-01-29 19:34:04	timed out waiting for media manager to mount volume
shivaji.vxindia.veritas.com	WorkGroup1	redalert.vxindia.veritas.com	52	2002-01-29 19:34:04	timed out waiting for media manager to mount volume

Media Errors Report

The *Media Errors* report provides a summary of all specific media-related problems that occurred during the selected reporting period. This report can help determine what media problems are occurring that are preventing NetBackup from completing the backup or restore activities.

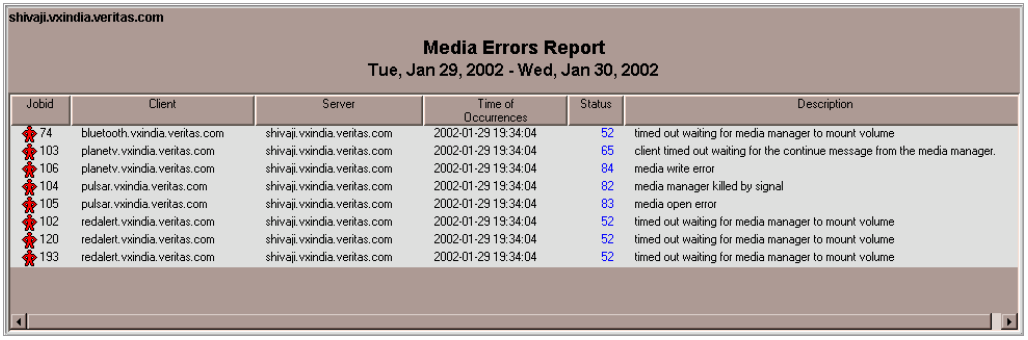
How to Access this Report

- Select the **Media Errors** option from the **Administrative** folder in the Report Generator window (restore data is displayed for jobs performed on the previous day)

Report Details

This report lists each server that had media-related problems, including the actual client that had the media problem. Click on the label for any field to sort entries by that field. Click on any entry in the **NetBackup Error Code** field to access the *NetBackup Trouble Shooting Guide*. For more information, see the "NetBackup Trouble Shooting Guide" on page 140.

Media Errors Report



shivaji.vxindia.veritas.com

Media Errors Report
Tue, Jan 29, 2002 - Wed, Jan 30, 2002

Jobid	Client	Server	Time of Occurrences	Status	Description
74	bluetooth.vxindia.veritas.com	shivaji.vxindia.veritas.com	2002-01-29 19:34:04	52	timed out waiting for media manager to mount volume
103	planetv.vxindia.veritas.com	shivaji.vxindia.veritas.com	2002-01-29 19:34:04	65	client timed out waiting for the continue message from the media manager.
106	planetv.vxindia.veritas.com	shivaji.vxindia.veritas.com	2002-01-29 19:34:04	84	media write error
104	pulsar.vxindia.veritas.com	shivaji.vxindia.veritas.com	2002-01-29 19:34:04	82	media manager killed by signal
105	pulsar.vxindia.veritas.com	shivaji.vxindia.veritas.com	2002-01-29 19:34:04	83	media open error
102	redalert.vxindia.veritas.com	shivaji.vxindia.veritas.com	2002-01-29 19:34:04	52	timed out waiting for media manager to mount volume
120	redalert.vxindia.veritas.com	shivaji.vxindia.veritas.com	2002-01-29 19:34:04	52	timed out waiting for media manager to mount volume
193	redalert.vxindia.veritas.com	shivaji.vxindia.veritas.com	2002-01-29 19:34:04	52	timed out waiting for media manager to mount volume

Restore Details by Client Report

The *Restore Details by Client* report provides details of all the restore jobs performed on the clients associated with the selected server.

This information may help you identify a client who is performing a number of restore jobs and investigate the reason why.

How to Access this Report

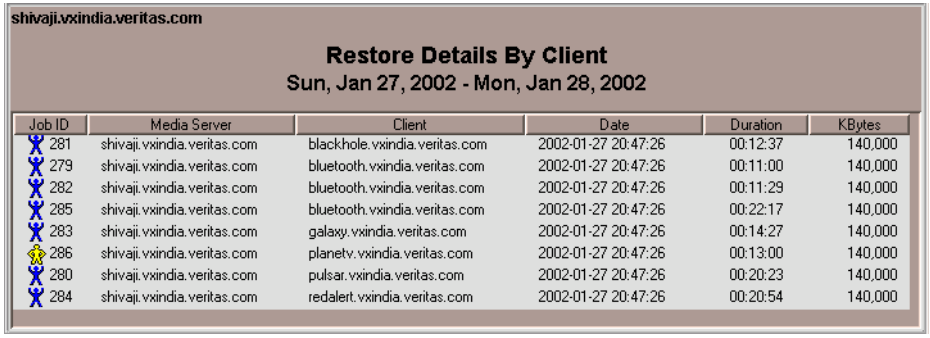
This report is generated by:

- Selecting the **Restore Details** option from the **Administrative** folder in the console tree (Restore data is displayed for jobs performed on the previous day.),
- Clicking on any bar in the *Restore Job Summary* report in the **Management** folder, or the *Restore Data Volumes* report (data displayed is for all restore jobs performed on the specific day selected), or

Report Details

This report lists the client's server where the files were restored; the date and time of the restoration; the duration of the job; and the size of the images read to complete the restore. Click on the label for any field to sort the entries by that field.

Restore Details by Client Report



shivaji.vxindia.veritas.com

Restore Details By Client

Sun, Jan 27, 2002 - Mon, Jan 28, 2002

Job ID	Media Server	Client	Date	Duration	KBytes
281	shivaji.vxindia.veritas.com	blackhole.vxindia.veritas.com	2002-01-27 20:47:26	00:12:37	140,000
279	shivaji.vxindia.veritas.com	bluetooth.vxindia.veritas.com	2002-01-27 20:47:26	00:11:00	140,000
282	shivaji.vxindia.veritas.com	bluetooth.vxindia.veritas.com	2002-01-27 20:47:26	00:11:29	140,000
285	shivaji.vxindia.veritas.com	bluetooth.vxindia.veritas.com	2002-01-27 20:47:26	00:22:17	140,000
283	shivaji.vxindia.veritas.com	galaxy.vxindia.veritas.com	2002-01-27 20:47:26	00:14:27	140,000
286	shivaji.vxindia.veritas.com	planetv.vxindia.veritas.com	2002-01-27 20:47:26	00:13:00	140,000
280	shivaji.vxindia.veritas.com	pulsar.vxindia.veritas.com	2002-01-27 20:47:26	00:20:23	140,000
284	shivaji.vxindia.veritas.com	redalert.vxindia.veritas.com	2002-01-27 20:47:26	00:20:54	140,000

Hosts under NetBackup Management Report

This report is a listing of all known hosts under the NetBackup management. A Host is considered any computer that has been backed up by the NetBackup application, also called a *client*.

Note This report may contain a lot of data, depending on the number of computers that are backed up by NetBackup.

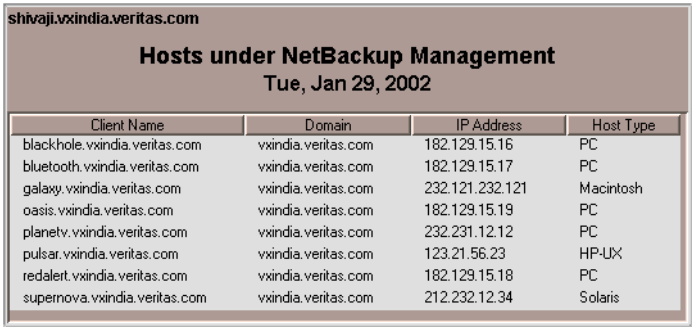
How to Access this Report

Select the **Host Listing** option from the **Administrative** folder.

Report Details

The *Hosts under NetBackup Management* report lists the name and IP address of each client, its domain and the type of machine.

Hosts under NetBackup Management Report



shivaji.vxindia.veritas.com

Hosts under NetBackup Management
Tue, Jan 29, 2002

Client Name	Domain	IP Address	Host Type
blackhole.vxindia.veritas.com	vxindia.veritas.com	182.129.15.16	PC
bluetooth.vxindia.veritas.com	vxindia.veritas.com	182.129.15.17	PC
galaxy.vxindia.veritas.com	vxindia.veritas.com	232.121.232.121	Macintosh
oasis.vxindia.veritas.com	vxindia.veritas.com	182.129.15.19	PC
planetv.vxindia.veritas.com	vxindia.veritas.com	232.231.12.12	PC
pulsar.vxindia.veritas.com	vxindia.veritas.com	123.21.56.23	HP-UX
redalert.vxindia.veritas.com	vxindia.veritas.com	182.129.15.18	PC
supernova.vxindia.veritas.com	vxindia.veritas.com	212.232.12.34	Solaris

Clients at Risk Report

This report identifies clients at risk based on the success of previous backups. Because the report's data depends on previous backups, only clients with at least one successful backup will be included. The report provides an analysis of the degree of success for each policy a client is a member of. The report is always generated for the current day because risk is calculated based on current conditions. To obtain detailed information about a particular client over the past month, click on an entry in the **Client Name** column to display the *Client Job History* report.

Note The *Client Job History* report displays the data collected for the month ending on the reference date. Examine this report to understand why a particular client is considered at risk currently.

How to Access this Report

Select the **Clients at Risk** option from the **Administrative** folder.

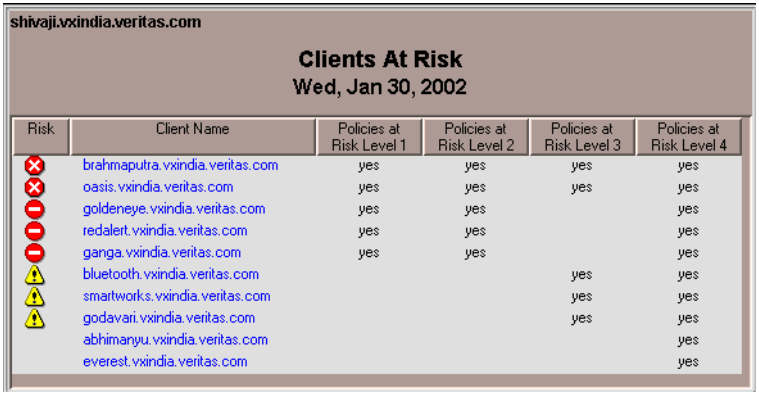
Report Details

The *Clients at Risk* report is a columnar report identifying clients at four risk levels. Whether or not a client is considered 'at risk' is determined by the success of the policies the client is part of. The meaning of each column is detailed below.

Column Name	Description
Risk	This column holds an overall risk rating icon. The clients listed are sorted on this column by default. The amount of risk is identified by the following icons.  .This icon displays if the client has a 'yes' value in 3 or 4 risk levels.  This icon displays if the client has a 'yes' value in 3 risk levels.  This icon displays if the client has a 'yes' value in 2 risk levels No icon displays if the client has only one risk level problem.
Client Name	The name of the client machine. This entry links to the *Client Job History* report for this client. The report displays the last month of data for this client. The number of clients in this report appears on the Health Panel in the *Site Summary* report. Reciprocally, the Clients at Risk entry on the Health Panel links to this report.

Column Name	Description
Policies at Risk Level 1	A ‘yes’ in this column indicates that the client is part of policies that were not successfully backed up in some user-defined number of days. The default is three days. You can set this value through the configuration utility.
Policies at Risk Level 2	A ‘yes’ in this column indicates the client is part of one or more policies for which the most recently run full backup was not successful.
Policies at Risk Level 3	A ‘yes’ in this column indicates the client is part of one or more policies for which the most recently run full backup was partially successful.
Policies at Risk Level 4	A ‘yes’ in this column indicates the client is part of one or more policies that use multistreaming, and that one or more of the streams failed.

Clients at Risk Report



shivaji.vxindia.veritas.com

Clients At Risk

Wed, Jan 30, 2002

Risk	Client Name	Policies at Risk Level 1	Policies at Risk Level 2	Policies at Risk Level 3	Policies at Risk Level 4
	brahmaputra.vxindia.veritas.com	yes	yes	yes	yes
	oasis.vxindia.veritas.com	yes	yes	yes	yes
	goldeneye.vxindia.veritas.com	yes	yes		yes
	redalert.vxindia.veritas.com	yes	yes		yes
	ganga.vxindia.veritas.com	yes	yes		yes
	bluetooth.vxindia.veritas.com			yes	yes
	smartworks.vxindia.veritas.com			yes	yes
	godavari.vxindia.veritas.com			yes	yes
	abhimanyu.vxindia.veritas.com				yes
	everest.vxindia.veritas.com				yes

Viewing the Media Reports 6

This chapter provides details on the *Media* reports available with VERITAS NetBackup Advanced Reporter 4.5 (NBAR).

Overview of the NBAR Media Reports

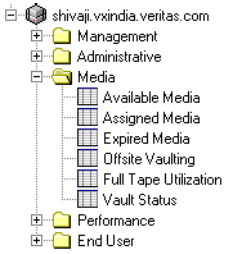
The Media reports generated by VERITAS NetBackup Advanced Reporter 4.5 provide information related to NetBackup's use of media. They also provide assistance in managing expired media and offsite vaulting.

Each Media report provides information on the current state of the NetBackup media. Unlike other NBAR reports, no historical information is kept. The Media reports include:

- *Available Media ("Available Media List"),*
- *Assigned Media ("Assigned Media List"),*
- *Expired Media ("Expired Media List"),*
- *Offsite Vaulting("Offsite Vaulting List"),*
- *Full Tape Utilization ("Full Tapes Utilization Report"), and*
- *Vault Status ("Current Vaulting Status Report")*

The following graphic displays all available Media reports.

Tree menu displaying Media reports



Available Media List

This report is a listing of all media available to the VERITAS Media Manager that are not assigned, that is, not in use by NetBackup. It does not include media that have been assigned but are expired.

Note This is not the same as the Media Lists report in NetBackup. That report includes media currently in use.

How to Access this Report

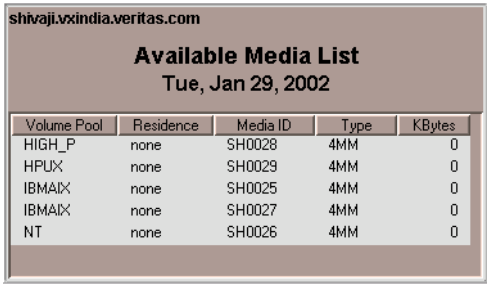
Select the **Available Media** option from the **Media** folder.

Report Details

The *Available Media List* displays the volume pool to which the media is assigned and the residence, or storage unit, the pool is assigned to. It also shows the media ID and type for each piece of media, and the amount of space which has been used. (If the media is available, the amount of space used should be zero.)

Click on the label for any field to sort the entries by that field.

Available Media List



Assigned Media List

This report is a listing of all media currently in use by NetBackup, including frozen media.

How to Access this Report

Select the **Assigned Media** option from the **Media** folder.

Report Details

The *Assigned Media List* displays the volume pool the media is assigned to, the media ID and media type. The date allocated is the date the media was first put into a volume pool. The retention level of the media is how long the images on this piece of media will be kept. Retention levels are configurable.

Click the label for any field to sort the entries by that field.

Assigned Media List

shivaji.vxindia.veritas.com

Assigned Media List
Tue, Jan 29, 2002

Volume Pool	Media ID	Type	Date Allocated	Retention Period	Expires On	Full ?	KBytes	Images
HIGH_P	SH0001	4MM	2002-01-25	1 week	2002-02-01	Yes	5,548,454	32,767
HIGH_P	SH0005	4MM	2002-01-27	1 week	2002-02-03	Yes	5,427,078	32,767
HIGH_P	SH0006	4MM	2002-01-23	1 week	2002-01-30	Yes	5,245,231	32,767
HIGH_P	SH0014	4MM	2002-01-25	1 week	2002-02-01	Yes	2,863,875	32,767
HIGH_P	SH0015	4MM	2002-01-27	1 week	2002-02-03	No	0	32,767
HIGH_P	SH0020	4MM	2002-01-26	1 week	2002-02-02	No	0	32,767
HPUX	SH0000	4MM	2002-01-26	1 week	2002-02-02	Yes	3,652,203	32,767
HPUX	SH0003	4MM	2002-01-24	1 week	2002-01-31	Yes	4,057,177	32,767
HPUX	SH0007	4MM	2002-01-24	1 week	2002-01-31	Yes	4,358,261	32,767
HPUX	SH0009	4MM	2002-01-27	1 week	2002-02-03	Yes	5,785,587	32,767
HPUX	SH0021	4MM	2002-01-26	1 week	2002-02-02	No	0	32,767
HPUX	SH0024	4MM	2002-01-23	1 week	2002-01-30	No	0	32,767
IBMAIX	SH0002	4MM	2002-01-27	1 week	2002-02-03	Yes	3,307,350	32,767
IBMAIX	SH0011	4MM	2002-01-26	1 week	2002-02-02	Yes	4,498,727	32,767
IBMAIX	SH0012	4MM	2002-01-22	1 week	2002-01-29	Yes	5,380,218	32,767
IBMAIX	SH0023	4MM	2002-01-24	1 week	2002-01-31	No	0	32,767
NetBackup	SH0016	4MM	2002-01-25	1 week	2002-02-01	No	0	32,767
NetBackup	SH0019	4MM	2002-01-25	1 week	2002-02-01	No	0	32,767
NT	SH0004	4MM	2002-01-26	1 week	2002-02-02	Yes	5,642,176	32,767
NT	SH0008	4MM	2002-01-23	1 week	2002-01-30	Yes	3,818,800	32,767
NT	SH0010	4MM	2002-01-23	1 week	2002-01-30	Yes	5,398,686	32,767
NT	SH0022	4MM	2002-01-22	1 week	2002-01-29	No	0	32,767
Solaris	SH0013	4MM	2002-01-26	1 week	2002-02-02	Yes	3,324,174	32,767
Solaris	SH0017	4MM	2002-01-24	1 week	2002-01-31	No	0	32,767
Solaris	SH0018	4MM	2002-01-27	1 week	2002-02-03	No	0	32,767

Expired Media List

This report lists all media that will expire on or before the selected date.

How to Access this Report

Select the **Expired Media List** option from the **Media** folder.

Report Details

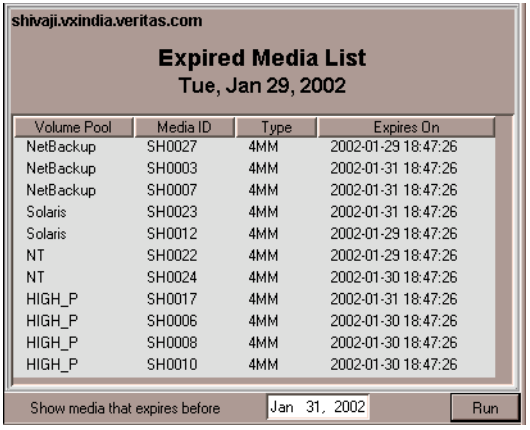
When you first access this report, NBAR displays the **Media expires before** date selector.

Media Expires Before Date Selector

Using the **Media expires before** date selector, select the date requested. You can change the date using the arrow keys on your computer's keyboard. Highlight the month, day or year you require and use the up or down keys to access the desired date. When you have the expiration date that you need, click the **Run** button.

The *Expired Media List* report then displays the list of media that will expire on or before the selected date.

Expired Media List



Offsite Vaulting List

This provides the user with the ability to list media that have been written to, in order to identify which media currently loaded in a storage device can be removed and stored and offsite. This procedure is called *vaulting*.

This report identifies tapes or other storage media either from a particular date range or within a particular policy or pool that have been written to and are candidates for offsite storage.

Note The information displayed in this report is not related to the NetBackup Vault option. The NetBackup Vault option generates a separate set of reports.

How to Access this Report

Select the **Offsite Vaulting** option from the **Media** folder.

Report Details

When you first access this report, NBAR displays the **Select from** selection criteria at the bottom of the *Offsite Vaulting List*.

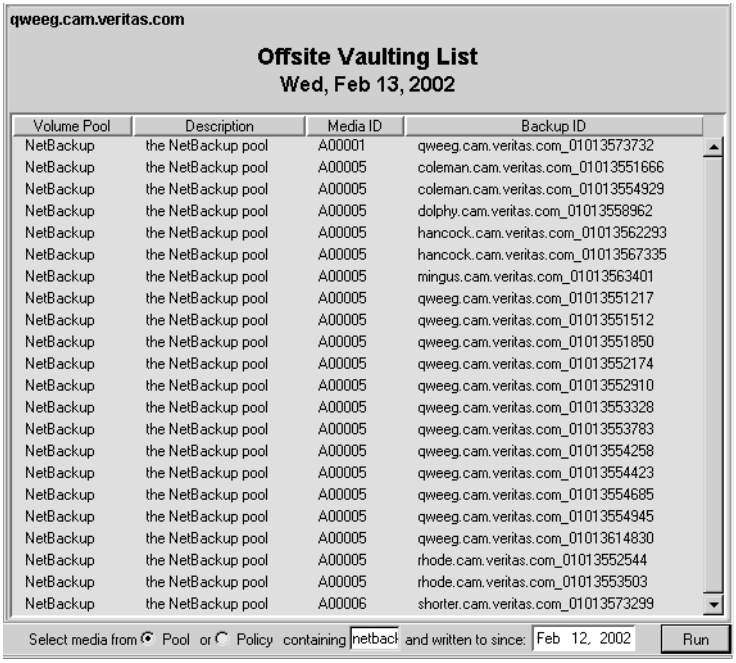
Offsite Vaulting List Report Selection Criteria

Follow the steps below to select criteria for a particular list.

1. Choose either the **Pool** or **Policy** radio buttons.
2. In the **containing** field, enter the name of a pool or the name of a policy. You can use a wildcard (%) as part of the name of either a pool or a policy. For example, **`%site`** will look for all media that is in a pool with a name ending with “site”. Similarly, **`%back%`** will match all names containing the word back.
3. Select the date requested (using the keyboard arrow keys, or typing in the new dates).
4. Click the **Run** button.

The *Offsite Vaulting List* then displays the available media based on the user’s selection criteria.

Offsite Vaulting List



qweeg.cam.veritas.com

Offsite Vaulting List
Wed, Feb 13, 2002

Volume Pool	Description	Media ID	Backup ID
NetBackup	the NetBackup pool	A00001	qweeg.cam.veritas.com_01013573732
NetBackup	the NetBackup pool	A00005	coleman.cam.veritas.com_01013551666
NetBackup	the NetBackup pool	A00005	coleman.cam.veritas.com_01013554929
NetBackup	the NetBackup pool	A00005	dolphy.cam.veritas.com_01013558962
NetBackup	the NetBackup pool	A00005	hancock.cam.veritas.com_01013562293
NetBackup	the NetBackup pool	A00005	hancock.cam.veritas.com_01013567335
NetBackup	the NetBackup pool	A00005	mingus.cam.veritas.com_01013563401
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013551217
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013551512
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013551850
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013552174
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013552910
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013553328
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013553783
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013554258
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013554423
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013554685
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013554945
NetBackup	the NetBackup pool	A00005	qweeg.cam.veritas.com_01013614830
NetBackup	the NetBackup pool	A00005	rhode.cam.veritas.com_01013552544
NetBackup	the NetBackup pool	A00005	rhode.cam.veritas.com_01013553503
NetBackup	the NetBackup pool	A00006	shorter.cam.veritas.com_01013573299

Select media from (•) Pool or ( ) Policy containing netbacl and written to since: Feb 12, 2002 Run

Full Tapes Utilization Report

This report lists the average amount of data stored on each full piece of media in each pool. This listing is intended to help you calculate the number of tapes you will need to fulfill your backup requirements.

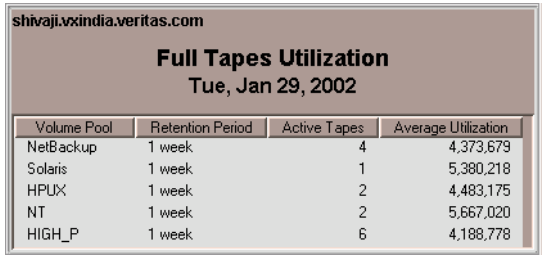
How to Access this Report

Select the **Full Tape Utilization** option from the **Media** folder.

Report Details

Only full tapes are included in this report. The **Average Utilization** field indicates the average amount of data on an active tape.

Tape Utilization Report



shivaji.vxindia.veritas.com

Full Tapes Utilization
Tue, Jan 29, 2002

Volume Pool	Retention Period	Active Tapes	Average Utilization
NetBackup	1 week	4	4,373,679
Solaris	1 week	1	5,380,218
HPUX	1 week	2	4,483,175
NT	1 week	2	5,667,020
HIGH_P	1 week	6	4,188,778

Current Vaulting Status Report

This report lists available media (media that contain images or have been written to) that are not currently loaded in a storage device.

Note The information displayed in this report is not related to the NetBackup Vault option. The NetBackup Vault option generates a separate set of reports.

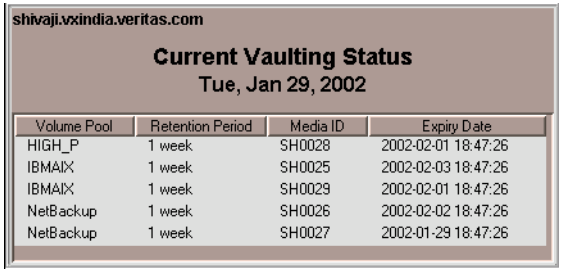
How to Access this Report

Select the **Vault Status** option from the **Media** folder.

Report Details

This report lists media not loaded in a storage device, while the *Offsite Vaulting List* lists media which are currently loaded in a storage device.

Current Vaulting Status Report



shivaji.vxindia.veritas.com

Current Vaulting Status

Tue, Jan 29, 2002

Volume Pool	Retention Period	Media ID	Expiry Date
HIGH_P	1 week	SH0028	2002-02-01 18:47:26
IBMAIX	1 week	SH0025	2002-02-03 18:47:26
IBMAIX	1 week	SH0029	2002-02-01 18:47:26
NetBackup	1 week	SH0026	2002-02-02 18:47:26
NetBackup	1 week	SH0027	2002-01-29 18:47:26

Viewing the Performance Reports 7

This chapter provides details on the Performance reports available with VERITAS NetBackup Advanced Reporter 4.5 (NBAR).

Overview of the NBAR Performance Reports

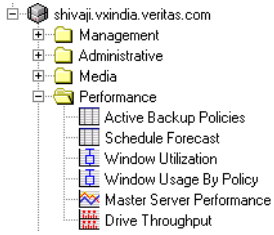
The Performance reports generated by VERITAS NetBackup Advanced Reporter 4.5 provide information related to the master server's performance. These reports allow the user to determine the performance quality of their systems. By viewing these reports, end users can note any anomalies that can then be reported to the appropriate System Administrator.

The reports in this chapter include:

- *Active Backup Policies ("Active Backup Policy Definitions Report"),*
- *Schedule Forecast ("Backup Job Schedule Forecast Report"),*
- *Window Utilization ("Window Utilization Report"),*
- *Window Usage by Policy ("Window Usage By Backup Policy Report"),*
- *Master Server Performance ("Master Server System Performance Report"),* and
- *Drive Throughput ("Drive Statistics Report").*

The following console tree displays all available Performance reports.

Tree menu displaying Performance reports



Active Backup Policy Definitions Report

This report is a listing of all active policies and their respective backup schedules for a particular date.

How to Access this Report

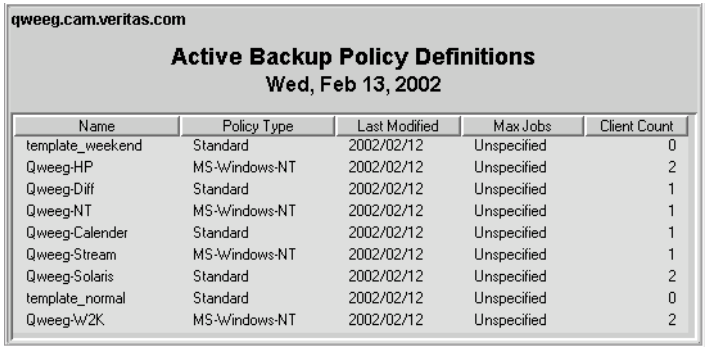
Select the **Active Policy Definitions** option from the **Performance** folder.

Report Details

For more detailed information about a particular policy, bring up the Policy Properties dialog box. To access Policy Properties, right-click on the name of the policy for which you want more information, and choose **Properties** from the context menu. The information about this policy found on the Policy Properties dialog is divided among four tabs: Schedules, Files, Clients, and Attributes. The Attributes tab only displays the attributes for this policy that NBAR collects.

Note The **Standard** policy type refers to UNIX clients.

Active Policy Definitions Report



qweeg.cam.veritas.com

Active Backup Policy Definitions
Wed, Feb 13, 2002

Name	Policy Type	Last Modified	Max Jobs	Client Count
template_weekend	Standard	2002/02/12	Unspecified	0
Qweeg-HP	MS-Windows-NT	2002/02/12	Unspecified	2
Qweeg-Diff	Standard	2002/02/12	Unspecified	1
Qweeg-NT	MS-Windows-NT	2002/02/12	Unspecified	1
Qweeg-Calender	Standard	2002/02/12	Unspecified	1
Qweeg-Stream	MS-Windows-NT	2002/02/12	Unspecified	1
Qweeg-Solaris	Standard	2002/02/12	Unspecified	2
template_normal	Standard	2002/02/12	Unspecified	0
Qweeg-W2K	MS-Windows-NT	2002/02/12	Unspecified	2

Backup Job Schedule Forecast Report

This report forecasts what backup jobs are scheduled to run in the next 24 hours. It gives specific date and time details for each job, as well as the number of clients scheduled.

This report tells you what types of backup jobs will run, categorized by policy and schedule.

How to Access this Report

Select the **Schedule Forecast** option from the **Performance** folder.

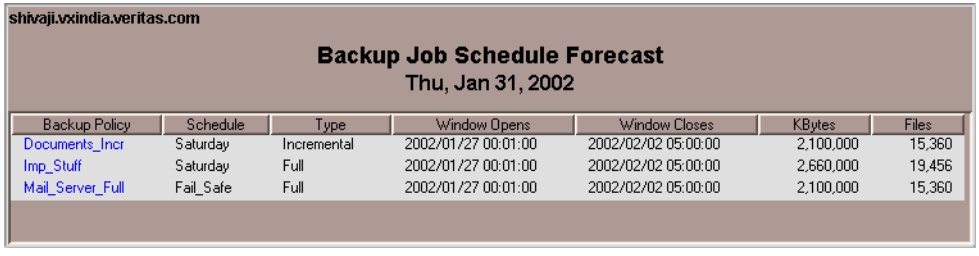
Report Details

To derive this forecast, the report looks at the previous week's activity for each active policy / schedule combination. To generate a meaningful forecast, historical data must be available. There are several conditions that must be met for data to appear on the report:

- NetBackup must have been running for at least six days.
- The database must be populated.
- Each policy must have been active for at least eight days.

Each entry in the **Policy** field links to a more detailed report. Click on any entry in the **Policy** field to access the "*Window Usage By Backup Policy Report*." report.

Backup Job Schedule Forecast Report



shivaji.vxindia.veritas.com

Backup Job Schedule Forecast

Thu, Jan 31, 2002

Backup Policy	Schedule	Type	Window Opens	Window Closes	KBytes	Files
Documents_Incr	Saturday	Incremental	2002/01/27 00:01:00	2002/02/02 05:00:00	2,100,000	15,360
Imp_Stuff	Saturday	Full	2002/01/27 00:01:00	2002/02/02 05:00:00	2,660,000	19,456
Mail_Server_Full	Fail_Safe	Full	2002/01/27 00:01:00	2002/02/02 05:00:00	2,100,000	15,360

Window Utilization Report

This report tells you how much time (in hours) has been used by each Policy's backup window during yesterday's jobs. It provides a clear graphical image of NetBackup activity.

How to Access this Report

Select the **Window Utilization** option from the **Performance** folder.

Report Details

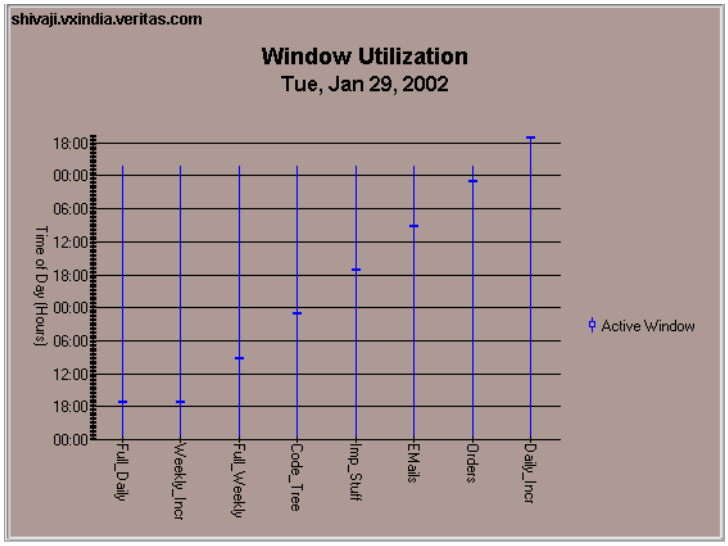
To derive this forecast, the report looks at the previous week's activity for each active policy / schedule combination. To generate a meaningful forecast, historical data must be available.

Note If NetBackup has not been running for at least six days, or if the database has not been populated, this report will not contain any data.

This report lists all backup windows use by policy (horizontal axis) and by time of day (vertical axis).

Each bar within this report links to a more detailed report for each specific day. When you click on any bar, the "*Window Usage By Backup Policy Report*" report appears displaying data for the selected policy.

Window Utilization Report



Window Usage By Backup Policy Report

This report reflects the schedule set for each policy by day. It can help you determine the average window utilization over time. The report also quickly highlights the possibility of any given schedule's windows becoming too small to support its workload.

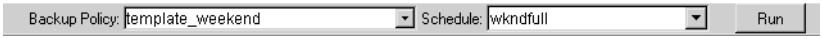
How to Access this Report

- Select the **Window Usage by Policy** option from the **Performance** folder or
- Click the **Policy** field in the *Backup Job Schedule Forecast* report or
- Click any bar in the *Window Utilization* report.

Report Details

When you first access this report, NBAR displays the **Policy** and **Schedule** selection criteria menu.

Policy and Schedule Selection Criteria



After selecting the appropriate policy and schedule using the pull down menu arrows, click the **Run** button (located further to the right) with your left mouse button to access the report.

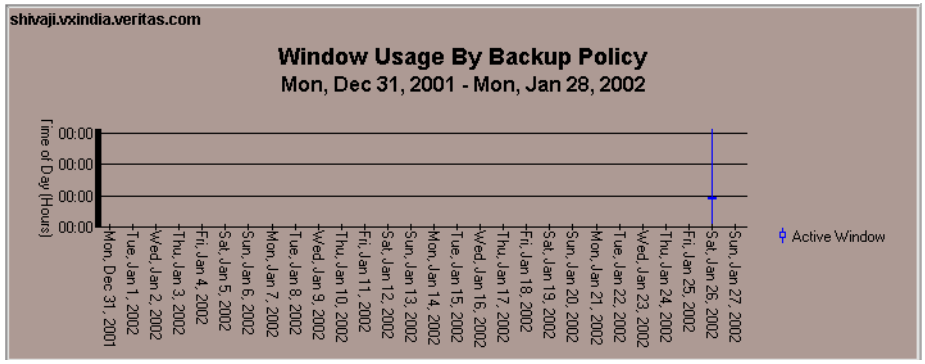
This report lists all window use for policy by day (horizontal axis) and by time of day in hours (vertical axis), and lets the user know how much time (in hours) has been used by each policy's backup window during yesterday's jobs. Backup window refers to the period of time during which backups can begin. This period of time may be cross-referenced with a particular NBU policy schedule.

Active backup window refers to the period of time during which the backups of a particular policy are active. The active backup window begins at the time that the first backup of a particular policy begins, and ends at the time that the last (remaining) active backup for a particular policy has completed.

Note If NetBackup has not been running for at least six days, or if the database has not been populated, this report will not contain any data.

Each bar within this report links to a more detailed report for each specific day. When you click on any bar, the "*Job Details for NetBackup Policy <policy name> Report*" report appears displaying backup data for the day selected.

Window Usage by Policy Report



Master Server System Performance Report

This report is a graph-based report that lets the user know how well their master server is operating. This report measures system performance through memory utilization (left vertical axis) and by how busy (in percent) the CPU is (right vertical axis) over time (horizontal axis). Memory utilization is represented by amount for Windows systems and by percentage in UNIX systems.

How to Access this Report

Select the **Master Server Performance** option from the **Performance** folder.

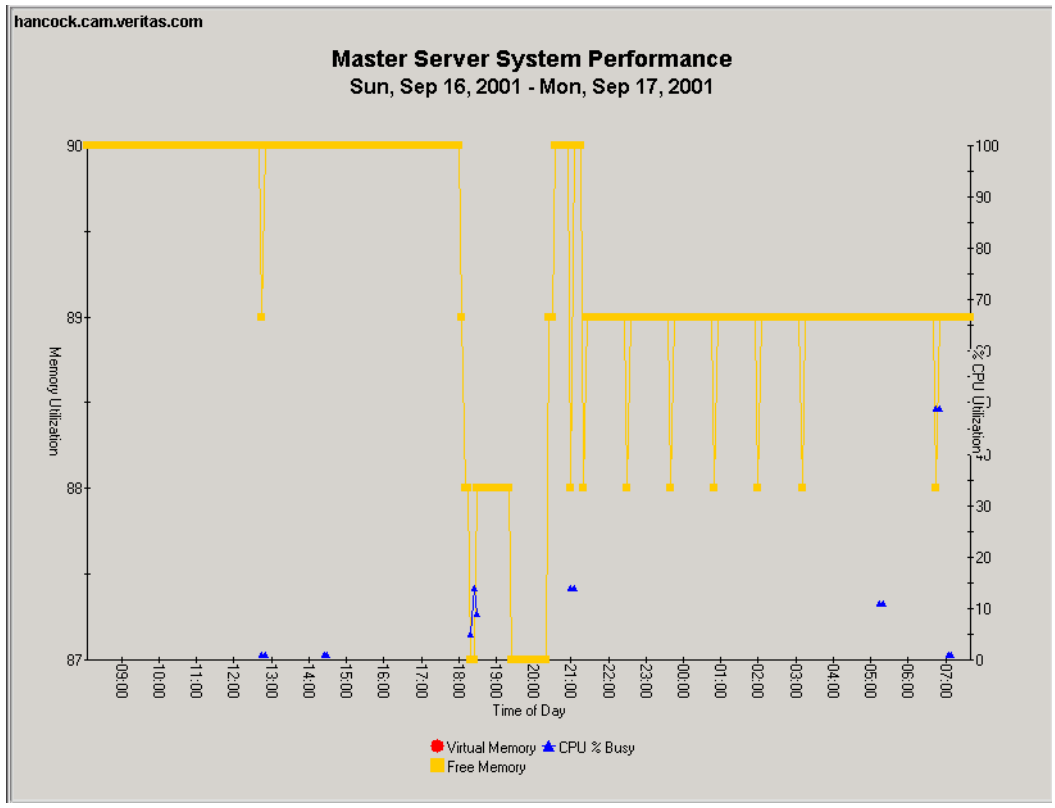
Report Details

Each graph line indicates a measure of performance:

- The red line is an indicator of Free Swap;
- the yellow line is an indicator of Free Memory;
- the blue line is an indication of how busy the CPU has been.

Note If there is not much activity for the master server depicted, the lines representing these data points look rough. The report generates a data point for every five minutes of the time period, which enables it to represent fine variations in a large amount of activity. Consequently, when there is little activity, the graph appears somewhat less sophisticated.

System Performance Report



Drive Statistics Report

This report plots the average data throughput and the number of jobs over a 24-hour period for the selected media server. You may want to run this report to get a sense of how much data each media server is processing. This report may also give you a sense of whether or not run times for the plotted jobs are balanced over the course of the reporting period.

How to Access the Report

Select the **Drive Throughput** option from the **Performance** folder.

Report Details

Use the media server selector to choose the media server you want to analyze.

Select Media Server Dialog Box

From the **Select media server** list box, choose the server you want to analyze. To select more than one server, hold down the Shift key as you highlight each server name. Click the **Run** button to generate a chart of server throughput performance.

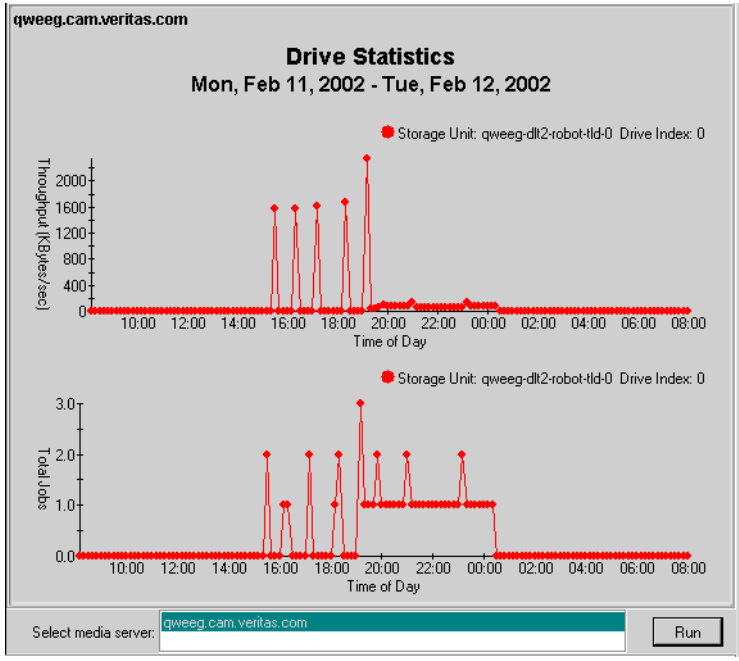
The upper chart displays the amount of data throughput over a 24-hour period for the media server selected.

Note The throughput values displayed in the drive statistics report may not match the throughput values displayed by the Activity Monitor. The Activity Monitor measures job duration as the time the job is active, while NBAR measures job duration only while the job is being written to tape for this report. This difference affects throughput calculations.

The lower chart displays the number of jobs over the course of the same 24 hours for the server.

Note The lower chart cannot be used to tally the number of jobs that ran during a specified time period. The points on the graph tell you the number of jobs that were running during the sampling time, but do not tell you whether each point represents a new job or continuation of a job.

Drive Statistics Report



Viewing the End User and Misc. Reports 8

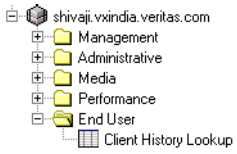
This chapter provides details on the *End User* report available with NBAR, titled, *Client Job History Report, and* on the Miscellaneous reports that can *only* be accessed through report links from other reports.

The Miscellaneous reports provide additional information in detail for certain reports. As a result, they do not appear on the report browser or the report menu. These reports are described only in this chapter, although they are accessed from a number of reports.

Overview of the End User Report

This report provides data on the backups for individual systems. It is accessible through the console tree.

Tree menu displaying the End User report



Client Job History Report

This feature of NBAR provides end users with information related to their own personal system's backup by allowing them to determine if their own critical data was backed up successfully. By viewing this report, end users can note any anomalies that can then be reported to the appropriate System Administrator. Additionally, this report allows an administrator to quickly view the backup information for a specific client.

How to Access this Report

Select the **Client History Lookup** option from the **End User** folder. You can also access this report from the *Clients at Risk* report. The *Clients at Risk* report provides an overview of backup success for all clients based on today's backup results.

Report Details

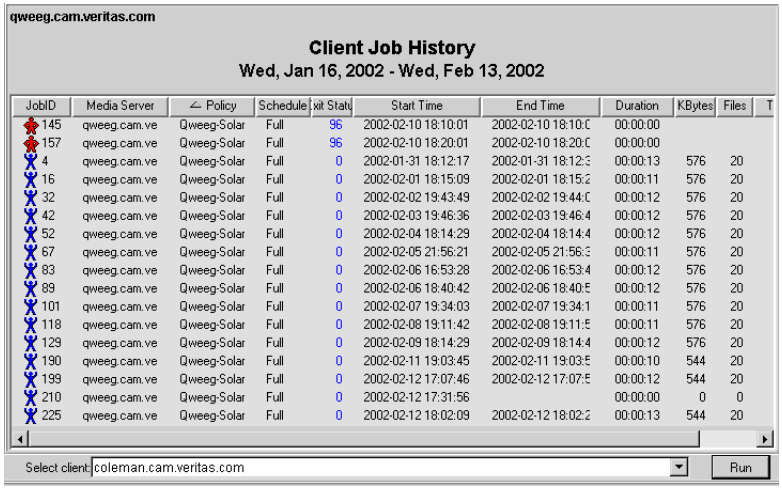
The *Client Job History* report lists all backup jobs performed on the end users machine during the last 28 day period. When you first access this report, NBAR displays the **Select client** pull down menu in the *Client Job History* report.

Select Client Pull Down Menu

Using the **Select client** pull down menu, select the name of the computer for which you want the job history, and click the **Run** button. Obtain a list of computer names by clicking on the **Select client** pull down menu arrow button. The **Select client** pull down menu remains at the bottom of the report allowing you to enter and view the information for another computer.

The *Client Job History* report then displays the information for the selected client. Click on any error entry in the **Status** field to access the *NetBackup Trouble Shooting Guide*. See the NetBackup Trouble Shooting Guide for more information.

Client Job History Report



qweeg.cam.veritas.com

Client Job History

Wed, Jan 16, 2002 - Wed, Feb 13, 2002

JobID	Media Server	Policy	Schedule	xit Statu	Start Time	End Time	Duration	KBytes	Files	T
145	qweeg.cam.ve	Qweeg-Solar	Full	96	2002-02-10 18:10:01	2002-02-10 18:10:0	00:00:00			
157	qweeg.cam.ve	Qweeg-Solar	Full	96	2002-02-10 18:20:01	2002-02-10 18:20:0	00:00:00			
4	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-01-31 18:12:17	2002-01-31 18:12:3	00:00:13	576	20	
16	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-01 18:15:09	2002-02-01 18:15:2	00:00:11	576	20	
32	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-02 19:43:49	2002-02-02 19:44:0	00:00:12	576	20	
42	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-03 19:46:36	2002-02-03 19:46:4	00:00:12	576	20	
52	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-04 18:14:29	2002-02-04 18:14:4	00:00:12	576	20	
67	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-05 21:56:21	2002-02-05 21:56:3	00:00:11	576	20	
83	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-06 16:53:28	2002-02-06 16:53:4	00:00:12	576	20	
89	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-06 18:40:42	2002-02-06 18:40:5	00:00:12	576	20	
101	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-07 19:34:03	2002-02-07 19:34:1	00:00:11	576	20	
118	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-08 19:11:42	2002-02-08 19:11:5	00:00:11	576	20	
129	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-09 18:14:29	2002-02-09 18:14:4	00:00:12	576	20	
190	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-11 19:03:45	2002-02-11 19:03:5	00:00:10	544	20	
199	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-12 17:07:46	2002-02-12 17:07:5	00:00:12	544	20	
210	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-12 17:31:56		00:00:00	0	0	
225	qweeg.cam.ve	Qweeg-Solar	Full	0	2002-02-12 18:02:09	2002-02-12 18:02:2	00:00:13	544	20	

Select client: coleman.cam.veritas.com Run

Overview of the NBAR Miscellaneous Reports

Miscellaneous reports are generated by VERITAS NetBackup Advanced Reporter 4.5 (NBAR) to provide more detail to individual backup reports. They can *only* be accessed through report links from other Management, Administrative and Performance reports. The reports in this chapter include the:

- "Summary of Status Code <number> Report",
- "Summary of Status Codes for <client> Report",
- "Summary of Status Code <number> for <client> Report",
- "NetBackup Trouble Shooting Guide", and
- "Job Details for NetBackup Policy <policy name> Report".

Summary of Status Code <*number*> Report

The purpose of this report is to provide a summary of the conditions under which a particular status code occurred.

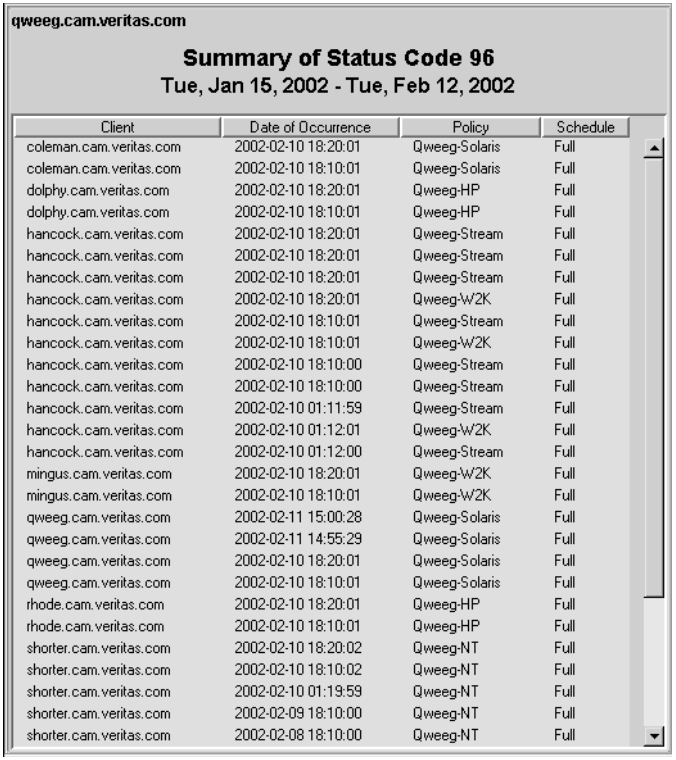
How to Access this Report

The *Summary of Status Code (number)* report is generated by clicking on any entry in the **Occurrences** field in the *Error Log Summary* report.

Report Details

This report provides a chronological list of every occurrence of a specific error code for the current time frame.

Summary of Status Code <*number*> Report



qweeg.cam.veritas.com

Summary of Status Code 96

Tue, Jan 15, 2002 - Tue, Feb 12, 2002

Client	Date of Occurrence	Policy	Schedule
coleman.cam.veritas.com	2002-02-10 18:20:01	Qweeg-Solaris	Full
coleman.cam.veritas.com	2002-02-10 18:10:01	Qweeg-Solaris	Full
dolphy.cam.veritas.com	2002-02-10 18:20:01	Qweeg-HP	Full
dolphy.cam.veritas.com	2002-02-10 18:10:01	Qweeg-HP	Full
hancock.cam.veritas.com	2002-02-10 18:20:01	Qweeg-Stream	Full
hancock.cam.veritas.com	2002-02-10 18:20:01	Qweeg-Stream	Full
hancock.cam.veritas.com	2002-02-10 18:20:01	Qweeg-Stream	Full
hancock.cam.veritas.com	2002-02-10 18:20:01	Qweeg-W2K	Full
hancock.cam.veritas.com	2002-02-10 18:10:01	Qweeg-Stream	Full
hancock.cam.veritas.com	2002-02-10 18:10:01	Qweeg-W2K	Full
hancock.cam.veritas.com	2002-02-10 18:10:00	Qweeg-Stream	Full
hancock.cam.veritas.com	2002-02-10 18:10:00	Qweeg-Stream	Full
hancock.cam.veritas.com	2002-02-10 01:11:59	Qweeg-Stream	Full
hancock.cam.veritas.com	2002-02-10 01:12:01	Qweeg-W2K	Full
hancock.cam.veritas.com	2002-02-10 01:12:00	Qweeg-Stream	Full
mingus.cam.veritas.com	2002-02-10 18:20:01	Qweeg-W2K	Full
mingus.cam.veritas.com	2002-02-10 18:10:01	Qweeg-W2K	Full
qweeg.cam.veritas.com	2002-02-11 15:00:28	Qweeg-Solaris	Full
qweeg.cam.veritas.com	2002-02-11 14:55:29	Qweeg-Solaris	Full
qweeg.cam.veritas.com	2002-02-10 18:20:01	Qweeg-Solaris	Full
qweeg.cam.veritas.com	2002-02-10 18:10:01	Qweeg-Solaris	Full
rhode.cam.veritas.com	2002-02-10 18:20:01	Qweeg-HP	Full
rhode.cam.veritas.com	2002-02-10 18:10:01	Qweeg-HP	Full
shorter.cam.veritas.com	2002-02-10 18:20:02	Qweeg-NT	Full
shorter.cam.veritas.com	2002-02-10 18:10:02	Qweeg-NT	Full
shorter.cam.veritas.com	2002-02-10 01:19:59	Qweeg-NT	Full
shorter.cam.veritas.com	2002-02-09 18:10:00	Qweeg-NT	Full
shorter.cam.veritas.com	2002-02-08 18:10:00	Qweeg-NT	Full

Summary of Status Codes for <*client*> Report

This report provides a chronological list of all errors that have occurred for the selected client.

How to Access this Report

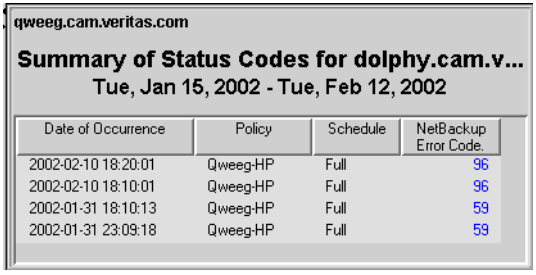
The *Summary of Status Codes for (Client)* report is generated by clicking on any entry in the **Client** field in the *Error Log Summary by Client* report (see the Error Log Summary by Client Report).

Report Details

The report contains the date the error occurred, the policy and schedule the error occurred in, and the NetBackup error code for the error.

Click on any entry in the **NetBackup Error Code** field to access the *NetBackup Trouble Shooting Guide* and a description of the error. See the NetBackup Trouble Shooting Guide.

Summary of Status Codes for <*client*> Report



Summary of Status Code <*number*> for <*client*> Report

This report provides details on the error selected from the *Error Log Summary by Client* report.

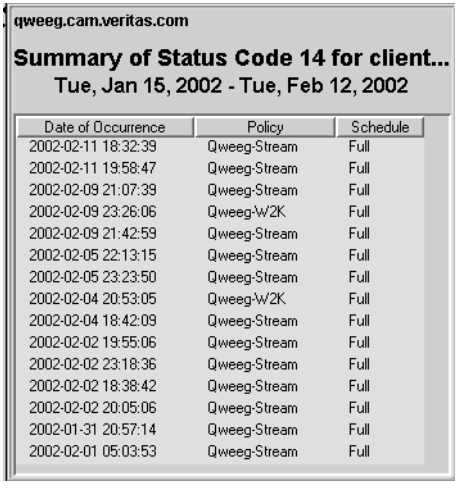
How to Access this Report

The *Summary of Status Code (number) for (Client)* report is generated by clicking on any entry in the **Occurrences** field in the *Error Log Summary by Client* report.

Report Details

This report included the name of the client that had the selected error, the date and time of each occurrence of the error, and the policy and schedule of the client at the time of the error.

Summary of Status Code <*number*> for <*client*> Report



qweeg.cam.veritas.com

Summary of Status Code 14 for client...

Tue, Jan 15, 2002 - Tue, Feb 12, 2002

Date of Occurrence	Policy	Schedule
2002-02-11 18:32:39	Qweeg-Stream	Full
2002-02-11 19:58:47	Qweeg-Stream	Full
2002-02-09 21:07:39	Qweeg-Stream	Full
2002-02-09 23:26:06	Qweeg-W2K	Full
2002-02-09 21:42:59	Qweeg-Stream	Full
2002-02-05 22:13:15	Qweeg-Stream	Full
2002-02-05 23:23:50	Qweeg-Stream	Full
2002-02-04 20:53:05	Qweeg-W2K	Full
2002-02-04 18:42:09	Qweeg-Stream	Full
2002-02-02 19:55:06	Qweeg-Stream	Full
2002-02-02 23:18:36	Qweeg-Stream	Full
2002-02-02 18:38:42	Qweeg-Stream	Full
2002-02-02 20:05:06	Qweeg-Stream	Full
2002-01-31 20:57:14	Qweeg-Stream	Full
2002-02-01 05:03:53	Qweeg-Stream	Full

NetBackup Trouble Shooting Guide

You can access the *NetBackup Trouble Shooting Guide* by clicking on any entry in the following fields:

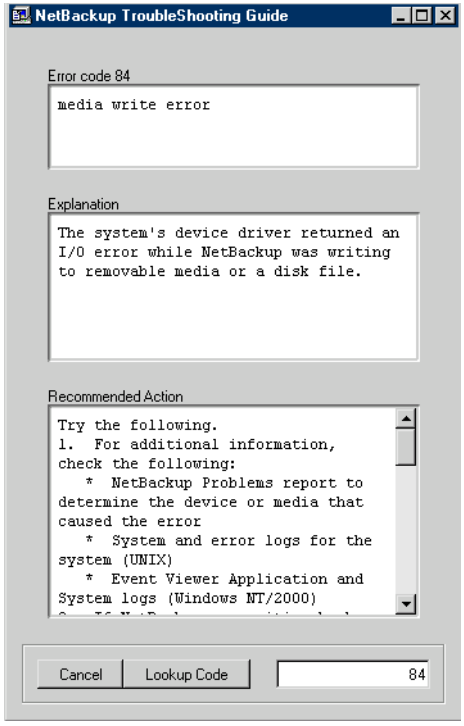
- the **Status** field of the *Error Log Summary* report, the *Error Log Summary by Client* report, the *Consolidated Error List* report, or the *Media Errors* report,
- the **NetBackup Error Code** field of the *Summary of Status Codes for (Client)* report,
- the **Exit Status** field of the *Site Details Job List* report, the *Job Details for NetBackup Policy (Policy name)* report, or the *Client Job History* report.

The *NetBackup Trouble Shooting Guide* provides the online Error code information. This information includes the Error code name and number, an Explanation of the error, the Recommended Action and a **Lookup Code** button and entry field. If you enter a code number in the field to the right, a description of the error will appear.

Beside the **Cancel** button is the **Lookup Code** button and an entry field to display or enter an Error code number. This button gives the user the ability to search for a specific error code. The Error code information is obtained by entering the applicable Error code number in the lower right entry field and clicking the [Lookup Code] button with the left mouse button. The *NetBackup Trouble Shooting Guide* will then display the online Error code information.

To exit this dialog box and return to the previously displayed report, click the **Cancel** button.

NetBackup Trouble Shooting Guide



Job Details for NetBackup Policy <*policy name*> Report

This report provides details on each backup job run for a selected Policy on the previous day.

How to Access this Report

Click any entry in the **Policy** report link in the *Backup Details by Policy* report, located in the **Administration** folder as the **Details by Policy** option.

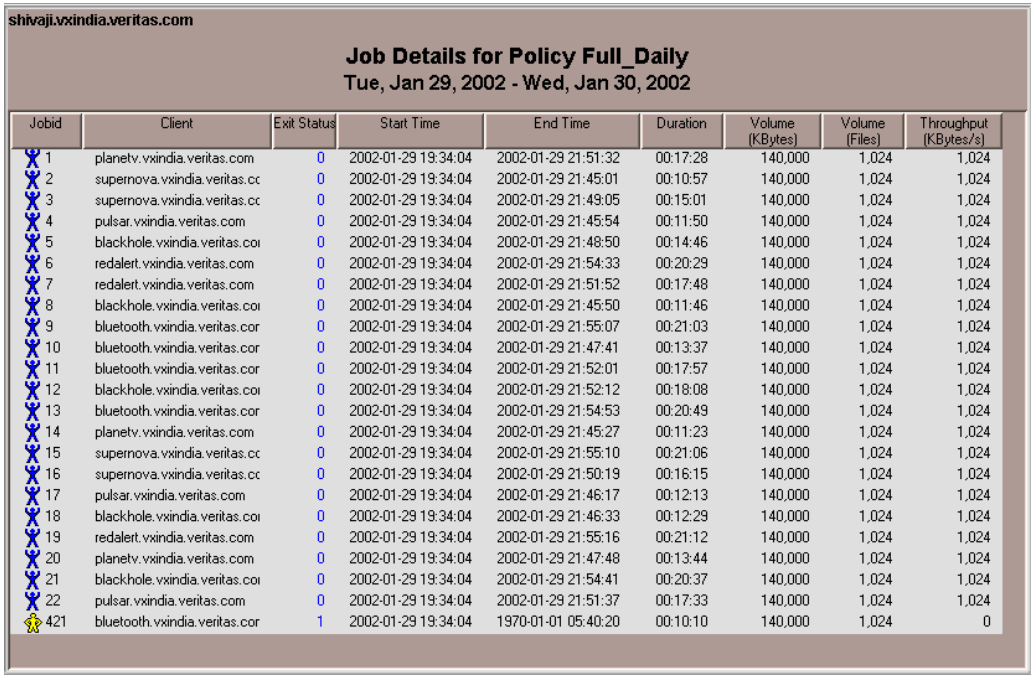
Report Details

If the backup job could not be completed, the **Exit Status** field will display an Error Status indicator with the applicable error number. Click on any Status entry in the **End Time** field to access the *NetBackup Trouble Shooting Guide*. See the NetBackup Trouble Shooting Guide.

Duration and **End Time** are defined slightly differently for successful jobs and failed jobs:

- For a successful job, **Duration** is the time it took the job represented by one job ID to complete, and **End Time** is the time the job ended.
- For a failed job, **Duration** is the time between the first time NetBackup tried to run the job, and the last time NetBackup tried to run the job. **End Time** for failed jobs is the last time the job was tried.

Job Details for NetBackup Policy <*policy name*> Report



shivaji.vxindia.veritas.com

Job Details for Policy Full_Daily

Tue, Jan 29, 2002 - Wed, Jan 30, 2002

Jobid	Client	Exit Status	Start Time	End Time	Duration	Volume (KBytes)	Volume (Files)	Throughput (KBytes/s)
1	planetv.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:51:32	00:17:28	140,000	1,024	1,024
2	supernova.vxindia.veritas.cc	0	2002-01-29 19:34:04	2002-01-29 21:45:01	00:10:57	140,000	1,024	1,024
3	supernova.vxindia.veritas.cc	0	2002-01-29 19:34:04	2002-01-29 21:49:05	00:15:01	140,000	1,024	1,024
4	pulsar.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:45:54	00:11:50	140,000	1,024	1,024
5	blackhole.vxindia.veritas.co	0	2002-01-29 19:34:04	2002-01-29 21:48:50	00:14:46	140,000	1,024	1,024
6	redalert.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:54:33	00:20:29	140,000	1,024	1,024
7	redalert.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:51:52	00:17:48	140,000	1,024	1,024
8	blackhole.vxindia.veritas.co	0	2002-01-29 19:34:04	2002-01-29 21:45:50	00:11:46	140,000	1,024	1,024
9	bluetooth.vxindia.veritas.cor	0	2002-01-29 19:34:04	2002-01-29 21:55:07	00:21:03	140,000	1,024	1,024
10	bluetooth.vxindia.veritas.cor	0	2002-01-29 19:34:04	2002-01-29 21:47:41	00:13:37	140,000	1,024	1,024
11	bluetooth.vxindia.veritas.cor	0	2002-01-29 19:34:04	2002-01-29 21:52:01	00:17:57	140,000	1,024	1,024
12	blackhole.vxindia.veritas.co	0	2002-01-29 19:34:04	2002-01-29 21:52:12	00:18:08	140,000	1,024	1,024
13	bluetooth.vxindia.veritas.cor	0	2002-01-29 19:34:04	2002-01-29 21:54:53	00:20:49	140,000	1,024	1,024
14	planetv.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:45:27	00:11:23	140,000	1,024	1,024
15	supernova.vxindia.veritas.cc	0	2002-01-29 19:34:04	2002-01-29 21:55:10	00:21:06	140,000	1,024	1,024
16	supernova.vxindia.veritas.cc	0	2002-01-29 19:34:04	2002-01-29 21:50:19	00:16:15	140,000	1,024	1,024
17	pulsar.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:46:17	00:12:13	140,000	1,024	1,024
18	blackhole.vxindia.veritas.co	0	2002-01-29 19:34:04	2002-01-29 21:46:33	00:12:29	140,000	1,024	1,024
19	redalert.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:55:16	00:21:12	140,000	1,024	1,024
20	planetv.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:47:48	00:13:44	140,000	1,024	1,024
21	blackhole.vxindia.veritas.co	0	2002-01-29 19:34:04	2002-01-29 21:54:41	00:20:37	140,000	1,024	1,024
22	pulsar.vxindia.veritas.com	0	2002-01-29 19:34:04	2002-01-29 21:51:37	00:17:33	140,000	1,024	1,024
421	bluetooth.vxindia.veritas.cor	1	2002-01-29 19:34:04	1970-01-01 05:40:20	00:10:10	140,000	1,024	0

Viewing the GDM Reports 9

This chapter describes the reports designed for multiple GDM managed servers, known as the GDM reports.

This chapter provides the following:

- A short discussion of relevant concepts
- A detailed description of each GDM report

Note In this chapter master servers that have NBAR installed are called GDM managed servers. The GDM master server with NBAR installed is called the GDM server (formerly known as the Master of Masters, or MoM).

If you are not certain that your environment has fulfilled the GDM prerequisites, please see "Planning for a GDM Configuration" on page 34. For further information, please refer to the NetBackup 4.5 DataCenter *System Administrator's Guide*.

GDM Concepts

In a GDM environment, each GDM managed server gathers information from the NetBackup catalog of the machine on which it is installed. Once in each 24-hour period each GDM managed server summarizes information from all of its clients and sends the data to the GDM master server. The process of collecting the data and passing it to the GDM master server is called a *rollup*. From the GDM master server you can access the GDM reports, which summarize information from all GDM managed servers.

Note Unlike the NBAR database on each managed server, which is seeded from NetBackup during installation, the GDM database will not contain data until the GDM server receives rolled up data from each managed server. By default, rollup occurs at 7:30 a.m. daily. The reports will not contain data until one day's worth of data has been rolled up. This means that if you set up your servers at 9 a.m. Monday, the first rollup will take place Tuesday morning. Therefore, GDM data will not display in your reports until after the rollup on Tuesday.

Glossary

Jobs in Progress

A *job in progress* is any job which is still running when the loader runs. A job in progress will not count towards the job tally for that day, but a count of jobs in progress is listed separately on the report to give you a sense of how many jobs are missing from the rollup totals.

Technically, a job in progress is a job which does not have a “0” or “1” exit status. All jobs in progress older than seven days are purged when the loader runs.

Loader

The *loader* is the NBAR process which collects data on each client from the NetBackup logs and adds it to the GDM managed server’s database. You can configure this process to run multiple times per day.

GDM Server

The *GDM server* is the server to which all GDM managed servers push the rolled up data from their clients. The GDM server must have NetBackup GDM software installed.

Rollup

A *rollup* is the process of collecting the data and passing it to the GDM server. Once in each 24-hour period each GDM managed server summarizes information from all of its clients and sends the data to the GDM server.

Rollup Time

The *rollup time* is the time each managed server begins to send its GDM data to the GDM server. This parameter is set in time local to the managed server, which is not necessarily the same as the time for the GDM server.

SORD

SORD is an acronym standing for *S*tart *O*f *R*eporting *D*ay. The SORD indicates the time at which a new reporting “day” (one 24-hour period) starts for each managed server (in local time). See “How NBAR Defines a Day” on page 146.

How NBAR Defines a Day

Each GDM managed server defines a ‘day’ as a 24-hour chunk of time for data collection purposes. For example, if you define the SORD as 8 am, than the ‘day’ is 8 am Monday - 7:59 am Tuesday. This GDM managed server day covers parts of two calendar days, but any job which starts before 8 am on a Tuesday is counted towards Monday’s activity because it falls within the same ‘day’ as defined by that server.

What If my GDM Managed Servers are in Different Time Zones?

If your servers are in different time zones, you need to think about the best time to run your GDM reports. In order to compile the most complete and accurate picture of the activity on your servers, the simplest approach is to set all SORDs to the same time and to make the westernmost server the GDM server. For example, if servers in all domestic USA time zones push their data to the GDM server at 8 am local time, data for all domestic time zones will be present. If the GDM server were in Boston, the administrator there wouldn't see complete GDM reports until 11 am.

Of course, each server's SORD may need to be different to reflect the backup schedules at each site. Or it may not be feasible for the westernmost server to be the GDM server. The following scenario describes a more complex configuration.

> Assume an GDM managed server in Portland, Maine and an GDM managed server in Portland, Oregon both set their SORD for 7 am. From the perspective of the GDM server, these servers start their days three hours apart, regardless of where the GDM server is located.
>
> Ideally, you will be able to schedule the rollup to the GDM server so that it occurs after the last SORD is defined.

The Scenario

There are four GDM managed servers: in Boston, Chicago, Minneapolis, and Los Angeles.

The server in Chicago (CST zone) is also the GDM server.

The local database is updated every hour on all of the servers.

The data is sent to the GDM server at the same time as the SORD.

The SORD is 7 am EST for the server in Boston.

The SORD is 1 pm CST for the server in Chicago.

The SORD is 7 am CST for the server in Minneapolis.

The SORD is 3 pm PST for the server in Los Angeles.

Note CST = EST - 1, PST = EST - 3

The Results

Time (EST)	Actions
6 am EST	The GDM managed servers update the local databases in Boston, Chicago, Minneapolis, and LA.
7 am EST	The GDM managed servers update the local databases in Boston, Chicago, Minneapolis, and LA. **BostonÕs daily rollup starts** The Boston GDM managed server connects to the GDM server and updates the GDM database with the data from this rollup.
8 am EST	The GDM managed servers update the local databases in Boston, Chicago, Minneapolis, and LA. **MinneapolisÕ daily rollup starts** The Minneapolis GDM managed server connects to the GDM server and updates the GDM database with the data from the most recent rollup.
9 am EST, and hourly until 6 pm EST	The GDM managed servers update the local databases in Boston, Chicago, Minneapolis, and LA.
2 pm EST	The GDM managed servers update the local databases in Boston, Chicago, Minneapolis, and LA. **ChicagoÕs daily rollup starts** The Chicago GDM managed server updates the GDM database with the data from the most recent rollup.
6 pm EST	The GDM managed servers update the local databases in Boston, Chicago, Minneapolis, and LA. **Los AngelesÕ daily rollup starts** The LA GDM managed server connects to the GDM server and updates the GDM database with the data from the most recent rollup.

The Conclusion

For this configuration, when you are looking at reports through the NBAR Java GUI, to get the most information from your reports, you would choose a reporting interval which starts sometime after 6 pm. That way, the report would summarize rollup information from all servers. If you ran a report and chose an interval which began before 6 pm, the

data from the GDM managed server in LA would not be represented accurately.

Note The reporting interval discussed above applies only to the reports you are generating. It is not related to the start-of-reporting-day that you configure for your servers.

GDM Summary Report Descriptions

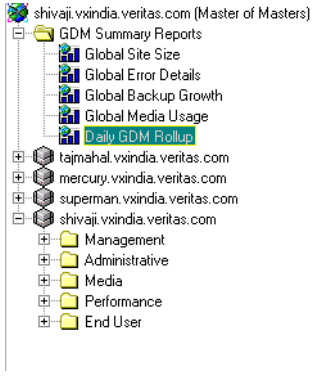
Each GDM summary report addresses a particular aspect of NetBackup backup activity on all the GDM managed servers on your network. Each report provides a way to compare the performance of the GDM managed servers on your network to each other, to pinpoint which sites are having problems with rollups or with storage space, and which sites are growing the fastest.

The GDM summary reports have all the features of the other NBAR reports, and provide additional information by including side notes in each report. The side note consists of a paragraph or so of descriptive text which displays next to the report. You can turn off the side notes by choosing **Hide Sidenotes** from the **View** menu.

GDM reports include:

- *Global Site Size* (“Global Site Size Report”),
- *Global Error Details* (“Global Error Details Report”),
- *Global Backup Growth* (“Global Backup Growth Report”)
- *Global Media Usage* (“Global Media Usage Report”), and
- *Daily GDM Rollup* (“Daily GDM Rollup Report”).

GDM Reports Tree



What are Tolerance Levels?

NBAR uses tolerance levels to determine when a GDM report value is unusual enough to flag or highlight for the user. For many of the GDM reports, there are tolerance levels preset in the nbar.conf file. These preset levels should work for most system configurations. However, if you want to change a tolerance level for any reason, please refer to "Administrative Tasks" on page 167

What Types of Information Do GDM Reports Contain?

This section outlines several ways in which you may find the information contained in the GDM reports useful.

- Assume that you have been tasked with projecting which sites in your GDM domain will require more backup hardware and backup media. Examine the Global Backup Growth report and the Global Media Usage report to determine which sites are growing the fastest, and which sites may be running out of media.
- Suppose that the Global Site Size report shows a managed server's NetBackup catalog growing exponentially. This could be consistent with the actual amount of data being backed up, or it could indicate a problem. Check the Global Backup Growth report for this server to see if the size of the catalog accurately reflects either the volume of data being backed up, or the number of files being backed up. If not, you may well have a problem and should investigate further.
- If a site is having many more media errors than average, the Global Error Details report will help you pinpoint the problem. An unusually large number of errors may indicate that you need to make more media available, or that you need to reconfigure NetBackup to use a different device to perform backups for this site.

Note You will not see any information on the GDM reports until one day of data has been collected. Depending on the time you set up the servers, this may take more than 24 hours.

Global Site Size Report

The GDM summary reports provide a synopsis of data from all GDM managed servers. This report contains information about how fast each site is growing, in terms of the number of backups performed by that site. This growth is measured by the size of the NetBackup catalog.

Purpose of this Report

This report lists information about the growth of the NetBackup catalog for each master server over the previous 12 month period. It's clear from the report which catalogs have had the fastest percentage growth.

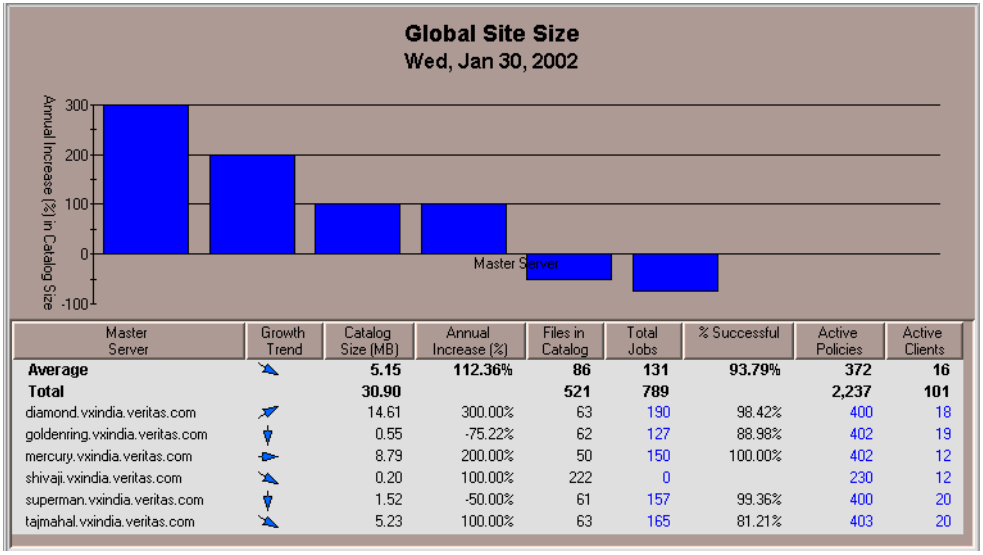
As with the other GDM reports, this report provides a tool for analyzing performance across your system and shows you the size of the catalog for each GDM managed server in relationship to the other GDM managed servers. The chart also provides information on the number of active policies and the number of active clients, so you can compare activity across servers.

Note The information for active policies and active clients fields is always based on data from the current day, regardless of the dates of the Global Site Size report. This is because data on active policies and clients is only available for policies and clients that are in use today.

How to Access this Report

Select the **Global Site Size** option from the **GDM Summary Reports** folder.

Global Site Size Report



Master Server	Growth Trend	Catalog Size (MB)	Annual Increase (%)	Files in Catalog	Total Jobs	% Successful	Active Policies	Active Clients
Average		**5.15**	**112.36%**	**86**	**131**	**93.79%**	**372**	**16**
Total		**30.90**		**521**	**789**		**2,237**	**101**
diamond.vxindia.veritas.com		14.61	300.00%	63	190	98.42%	400	18
goldenring.vxindia.veritas.com		0.55	-75.22%	62	127	88.98%	402	19
mercury.vxindia.veritas.com		8.79	200.00%	50	150	100.00%	402	12
shivaji.vxindia.veritas.com		0.20	100.00%	222	0		230	12
superman.vxindia.veritas.com		1.52	-50.00%	61	157	99.36%	400	20
tajmahal.vxindia.veritas.com		5.23	100.00%	63	165	81.21%	403	20

Report Details

This section explains the data displayed in the graphical chart and in the table.

Bar Chart

The Global Site Size chart displays the annual percentage of growth for each GDM managed server's catalog.

Each vertical bar represents one GDM managed server. Allow the cursor to hover on a selected bar to see the name of the GDM managed server and the percent change from one year ago.

Column Name	Description
Master Server	The GDM managed server which is this site's master server.

Column Name	Description
Growth Trend	A visual indication of how fast this site's catalog is growing. There are five indicators:  increasing a lot  increasing some  staying about the same  decreasing some  decreasing a lot
Catalog Size	The actual size of the catalog on the date of this report.
Annual Increase (%)	The percentage change in the size of the catalog compared to the same date 12 months ago. If there are not 12 months of data, NBAR uses the earliest date.
Files in Catalog	The number of files in the catalog on the report date.
Total Jobs	The total number of jobs that were run the previous day on this server. This field links to the *Detailed Job List* report for this server.
%Successful	The percentage of jobs that succeeded.
Active Policies	The total number of active policies for this server's backups. This field links to the *Active Policy Definitions* report for this server. **Note** The information for this field is always based on data from the current day, regardless of the dates of the Global Site Size report.

Column Name	Description
Active Clients	The total number of clients in active policies that are being backed up by this server. This field links to the *Hosts under NetBackup Management* report for this server. **Note** The information for this field is always based on data from the current day, regardless of the dates of the Global Site Size report.

Global Error Details Report

The GDM summary reports provide a synopsis of data from all GDM managed servers. This report contains information about each server's problems.

Purpose of this Report

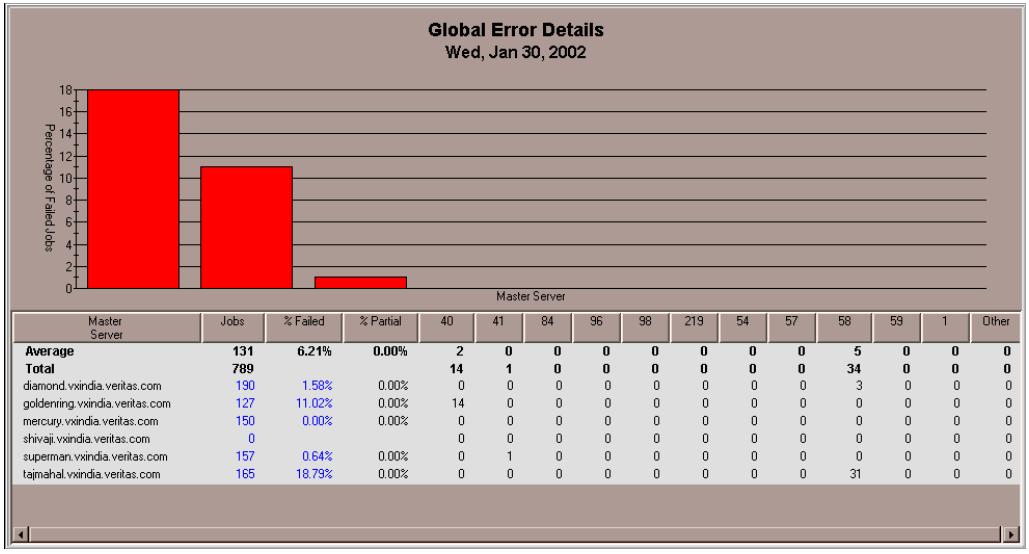
This report lists information about the failed jobs for each GDM managed server over a specified period of time. It's clear from the report which servers are having the most trouble, as indicated by the percentage of failed jobs, and which errors (by error code) occur most frequently.

As with the other GDM reports, this report provides a tool for analyzing NBAR backup performance across your system and shows you the performance of each GDM managed server in relationship to the other GDM managed servers.

How to Access this Report

Select the **Global Error Details** option from the **GDM Summary Reports** folder.

Global Error Details Report



Master Server	Jobs	% Failed	% Partial	40	41	84	96	98	219	54	57	58	59	1	Other
Average	**131**	**6.21%**	**0.00%**	**2**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**5**	**0**	**0**	**0**
Total	**789**			**14**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**34**	**0**	**0**	**0**
diamond.vxindia.veritas.com	190	1.58%	0.00%	0	0	0	0	0	0	0	0	3	0	0	0
goldenring.vxindia.veritas.com	127	11.02%	0.00%	14	0	0	0	0	0	0	0	0	0	0	0
mercury.vxindia.veritas.com	150	0.00%	0.00%	0	0	0	0	0	0	0	0	0	0	0	0
shivaji.vxindia.veritas.com	0			0	0	0	0	0	0	0	0	0	0	0	0
superman.vxindia.veritas.com	157	0.64%	0.00%	0	1	0	0	0	0	0	0	0	0	0	0
tajmahal.vxindia.veritas.com	165	18.79%	0.00%	0	0	0	0	0	0	0	0	31	0	0	0

Report Details

This section explains the data displayed in the graphical chart and in the table.

Bar Chart

The Global Error Details chart displays the percentage of failed jobs for each GDM managed server for the time frame specified for this report.

Each vertical bar represents one GDM managed server. Hover the cursor over a selected bar to see the name of the GDM managed server and the percentage of jobs which failed. Click on the bar to bring up the *Error Log Summary* report for that server.

Column Name	Description
Server	The name of the NBAR managed server on which the jobs ran.
Jobs	The number of jobs that ran during the report's time period. Click on this entry to bring up the *Detailed Job List* for this GDM managed server.
%Failed	The percentage of all jobs run during the report's time period that failed. For this report, a job is classified as "failed" if it fails during the last attempt, not if it failed on an initial attempt, but eventually succeeded on a retry. Click on this entry to bring up the *Consolidated Error List* for this GDM managed server.
%Partial	The percentage of jobs that were partially successful.
Error Codes	The number of jobs that failed due to the error represented by the error code in the column header.
1	An error code of 1 indicates that the job was partially successful. This entry is the number of jobs that were partially successful during the time frame of this report.
Other	The number of jobs that failed because of less common errors. A job counts as failed if the last attempt failed.

Error Tolerance Levels

The error tolerance level is a level of occurrences of a particular error code above which the server in question may experience serious problems. The entries for the %Failed and the Error Code columns will be highlighted if their values exceed the specified limit. The error tolerance levels are preset, but are configurable through the configuration utility. See the chapter "Administrative Tasks" for details.

Global Backup Growth Report

The GDM summary reports provide a synopsis of data from all GDM managed servers. This report contains information about how fast each site is growing, in terms of amount of data backed up.

Purpose of this Report

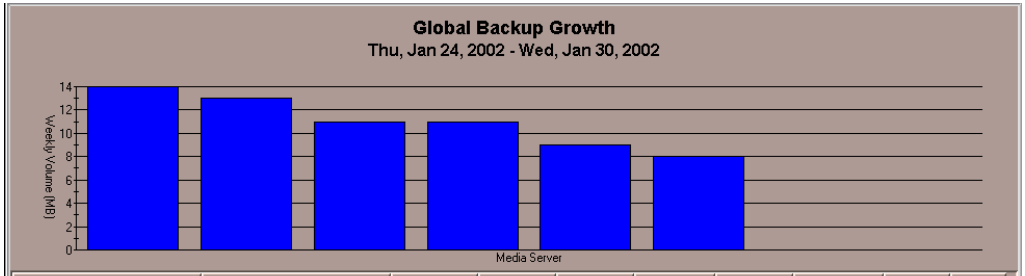
This report lists information about the increase in weekly volume of backups for each media server compared with an earlier week. It's clear from the report which media servers have had the largest increase in backup volume.

As with the other GDM reports, this report provides a tool for analyzing performance across your system. It demonstrates the volume of backups for each media server in relationship to the other media servers. The chart also provides information on the number of storage units and drives used by each media server.

How to Access this Report

Select the **Global Backup Growth** option from the **GDM Summary Reports** folder.

Global Backup Growth Report



Master Server	Media Server	Weekly Volume (MB)	%Changed	Annual %Changed	Files	%Changed	Annual %Changed	Storage Units	Drives
Average		**11.66**	**0.00%**	**0.00%**	**12,000**	**0.00%**	**300.00%**	**70**	**9**
Total		**69.97**			**72,000**			**420**	**54**
diamond.vxindia.veritas.com	diamond.vxindia.veritas.com	8.94	0.00%	0.00%	12,000	0.00%	300.00%	70	9
goldenring.vxindia.veritas.com	goldenring.vxindia.veritas.com	9.73	0.00%	0.00%	12,000	0.00%	300.00%	70	9
mercury.vxindia.veritas.com	mercury.vxindia.veritas.com	13.03	0.00%	0.00%	12,000	0.00%	300.00%	70	9
shivaji.vxindia.veritas.com	shivaji.vxindia.veritas.com	11.49	0.00%	0.00%	12,000	0.00%	300.00%	70	9
superman.vxindia.veritas.com	superman.vxindia.veritas.com	14.82	0.00%	0.00%	12,000	0.00%	300.00%	70	9
tajmahal.vxindia.veritas.com	tajmahal.vxindia.veritas.com	11.96	0.00%	0.00%	12,000	0.00%	300.00%	70	9

Report Details

This section explains the data displayed in the graphical chart and in the table.

Bar Chart

The Global Backup Growth chart displays the weekly backup volume for each media server. Hover the cursor over a selected vertical bar to display the name of the server, the amount of data backed up, and the change from a previous week. The red portion of each bar indicates the change over a previous week.

Note The tooltip dates will not reflect whole successive weeks if data is not available for the entire week used to compare to the week beginning with the reference date. Instead, the first week will begin with the earliest date for which data is available, potentially resulting with an overlap with the week defined by the reference date.

Table

The **annual percentage change** field in the table compares the data for the week beginning with the reference date to the same week a year ago to determine the annual percentage change for backups. If a year's worth of data is not available, the comparison will be made to the earliest week for which data is available.

The **percentage change** field in the table always compares the data for the week beginning with the reference date to the first week in the report's time frame irrespective of data being available. If data is not available for that first week, some table entries will be blank.

Column Name	Description
Master Server	The GDM managed server to which the media server sends its images.
Media Server	The media server that performs the backups.
Weekly Volume	The volume of data backed up by the media server from six days prior to the end date of the report and including the end date of the report.
%Changed	The percentage change in the amount of data backed up by the media server from the first week this report covers to the last week this report covers.

Column Name	Description
Annual %Changed	The percentage change in the weekly volume of data backed up by this media server compare to the weekly volume backed up by this media server one year ago. If the report data does not go back a year, the earliest week's worth of available data is used. **Note** Entries with a ⚠ symbol and highlighted in color indicate that the annual percent changed value for this media server is far higher than the average.
Files	The number of files backed up by the given media server on the end date and the six days prior to the end date.
%Changed	The percentage change between the number of files backed up by this media server from the first week in the reporting period to the last week in the reporting period.
Annual %Changed	The percentage change in the number of files backed up by this media server for this reporting period compared to this period one year ago.
Storage Units	The number of storage units which are defined on this media server on the end date of this reporting period.
Drives	The number of drives connected to this media server on the end date of this reporting period.

Tolerance Levels

NBAR sets a default tolerance level for the Annual %Change value. The entries for this field will be highlighted if they exceed this value. If necessary, you can change this value through the configuration utility. Please see the chapter "Administrative Tasks" for more details.

Global Media Usage Report

The GDM summary reports provide a synopsis of data from all NBAR servers. This report summarizes media usage for each media server on your system and tries to answer the questions: Do I have slots in my robot? Where can I recycle tapes?

Purpose of this Report

This report provides information on the status of the media available to each media server on your system.

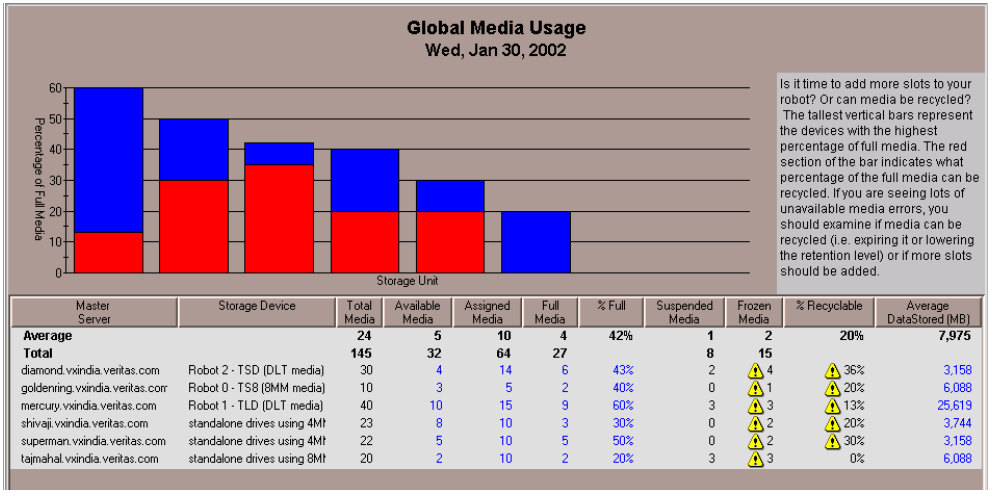
As with the other GDM reports, this report provides a tool for analyzing performance across your system and highlights GDM managed servers which may be running low on backup media. The chart also provides information on the percentage of recyclable media, suspended media, and frozen media for each storage unit.

The goal of the data displayed here is to get a sense of whether you can recycle enough media to fulfill your storage needs, or whether you need to add drives to your storage system.

How to Access this Report

Select the **Global Media Usage** option from the **GDM Summary Reports** folder.

Global Media Usage Report



Master Server	Storage Device	Total Media	Available Media	Assigned Media	Full Media	% Full	Suspended Media	Frozen Media	% Recyclable	Average DataStored (MB)
Average		**24**	**5**	**10**	**4**	**42%**	**1**	**2**	**20%**	**7,975**
Total		**145**	**32**	**64**	**27**		**8**	**15**		
diamond.vxindia.veritas.com	Robot 2 - TSD (DLT media)	30	4	14	6	43%	2	⚠ 4	⚠ 36%	3,158
goldenring.vxindia.veritas.com	Robot 0 - TS8 (8MM media)	10	3	5	2	40%	0	⚠ 1	⚠ 20%	6,088
mercury.vxindia.veritas.com	Robot 1 - TLD (DLT media)	40	10	15	9	60%	3	⚠ 3	⚠ 13%	25,619
shivaji.vxindia.veritas.com	standalone drives using 4Mf	23	8	10	3	30%	0	⚠ 2	⚠ 20%	3,744
superman.vxindia.veritas.com	standalone drives using 4Mf	22	5	10	5	50%	0	⚠ 2	⚠ 30%	3,158
tajmahal.vxindia.veritas.com	standalone drives using 8Mf	20	2	10	2	20%	3	⚠ 3	0%	6,088

Report Details

This section explains the data displayed in the graphical chart and in the table.

Bar Chart

The Global Media Usage chart displays the percentage of full media for each media server.

Each vertical bar represents the media assigned to a particular media server. Hover with the cursor over each vertical bar to see the name of the media server, the percentage of full media and what percentage of media can be recycled. The section of each bar in red represents the portion of the full media for that media server that can be recycled.

Column Name	Description
Master Server	The NBAR managed server which is this site's master server.
Storage Device	This field both identifies the storage device and indicates what type of media is being used. For example, if the storage device is a robot, and it contains some drives which handle 4 mm tape and some which handle 8 mm tape, then that robot will have two entries here - robot - 4 mm and robot - 8 mm.
Total Media	The number of media that are currently configured in the storage device. If this is a multimedia device, the total media will apply only to one type of media. For example, if the device contains 4 4mm drives and 4 8 mm drives, than this device will be represented by two rows, and the entry under Total Media will be 4 for both rows.
Available Media	The number of media that are not currently assigned for use by NetBackup. This field links to the *Available Media List* for the selected GDM managed server.
Assigned Media	The number of media that are currently in use by NetBackup. This field links to the *Assigned Media List* for this GDM managed server.
Full Media	The number of assigned media which are full. This field links to the *Assigned Media List* for this GDM managed server.

Column Name	Description
%Full	The percentage of assigned media which are full. This field links to the *Assigned Media List* for this GDM managed server.
Suspended Media	The number of media which are currently suspended.
Frozen Media	The number of media which are frozen.
%Recyclable	The percentage of media which could be recycled. The conditions which make a piece of media eligible for recycling are either: ◆ media is full but not expired (that is, inactive) and ◆ the retention level is set for more than a month from the date of this report. The retention level at which NBAR considers a tape potentially inactive is preset for 30 days.
Average Data Stored	The average amount of data stored on each full piece of media for this GDM managed server. This field links to the *Full Tapes Utilization* report for this GDM managed server.

Retention Level

NBAR sets a default retention level of 30 days. If you must change this parameter, you can do so through the configuration utility. Please see the chapter "Administrative Tasks" for more details.

Daily GDM Rollup Report

The GDM summary reports provide a synopsis of data from all GDM managed servers. This report contains information about each server's rollup activity.

Purpose of this Report

This report lists information about the about GDM rollup activity from each GDM managed server to the GDM server. The report highlights any servers that have not completed a successful rollup in the last 24 hours. The report also displays information on how long the rollup took, and an estimate of when the next rollup will occur for each server.

As with the other GDM reports, this report provides a tool for analyzing NBAR rollup performance across your system. This report shows you the status of your rollups in the GDM environment.

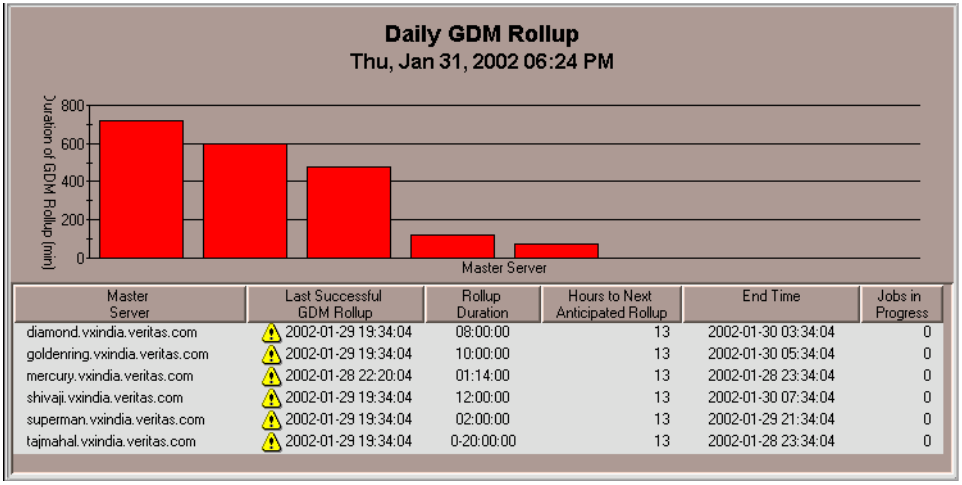
You can see at a glance if all rollups have completed successfully, how much time each rollup is taking, and if there were jobs in progress when GDM data collection occurred.

Note If the Daily GDM Rollup report indicates that a GDM managed server has not rolled up properly, then you must assume that any data compiled from all servers that appears in the GDM reports might be inaccurate.

How to Access this Report

Select the **Daily GDM Rollup** option from the **GDM Summary Reports** folder. This report does not link to any others.

Daily GDM Rollup Report



Master Server	Last Successful GDM Rollup	Rollup Duration	Hours to Next Anticipated Rollup	End Time	Jobs in Progress
diamond.vxindia.veritas.com	2002-01-29 19:34:04	08:00:00	13	2002-01-30 03:34:04	0
goldenring.vxindia.veritas.com	2002-01-29 19:34:04	10:00:00	13	2002-01-30 05:34:04	0
mercury.vxindia.veritas.com	2002-01-28 22:20:04	01:14:00	13	2002-01-28 23:34:04	0
shivaji.vxindia.veritas.com	2002-01-29 19:34:04	12:00:00	13	2002-01-30 07:34:04	0
superman.vxindia.veritas.com	2002-01-29 19:34:04	02:00:00	13	2002-01-29 21:34:04	0
tajmahal.vxindia.veritas.com	2002-01-29 19:34:04	0-20:00:00	13	2002-01-28 23:34:04	0

Report Details

This section explains the data displayed in the graphical chart and in the table.

Bar Chart

The Daily GDM Rollup chart displays the amount of time the most recent rollup took for each NBAR managed server. This value is calculated from the time each server began sending information to the GDM server until all the information has been processed and stored by the GDM server. Hover the cursor over a selected vertical bar to see the server name and the time needed for the last rollup.

If the server which sent the rolled up data is represented in red, that means the GDM server has not received a rollup from that server for over 24 hours, and there may be a problem with the server.

Column Name	Description
Server	The name of the NBAR managed server that rolls up the data to the GDM server.

Column Name	Description
Last Successful GDM Rollup	The time and day the GDM managed server began the rollup process and the GDM server began receiving rollup data. The time in this field is in the GDM server's time zone, not the time zone of the GDM managed server. A ⚠ symbol next to an entry indicates that a successful rollup has not occurred in the past 24 hours.
Rollup Duration	The amount of time (hours:minutes:seconds) between when the GDM server began receiving data from the rollup and when the GDM server finished processing the data.
Hours to Next Anticipated Rollup	The number of hours until the GDM server expects to begin receiving data for the next scheduled rollup from this server. This number represents, to the nearest hour, the number of hours from the time this report is generated until the next scheduled rollup. Rollup time defaults to 7:30 a.m.
End Time	The time at which the GDM server finished storing the data from the most recent rollup for this server.
Jobs in Progress	The number of jobs which were not completed at the time the server collected the GDM rollup data. These jobs will be picked up the next time rollup data is collected.

Administrative Tasks 10

This chapter explains the procedures for administrative tasks in NBAR.

When you are finished with chapter, you will know how to:

- Start NBAR for the first time
- Use the Configuration Utility
- Use the Export Utility
- Find more information on NBAR's database

Starting VERITAS NetBackup Advanced Reporter 4.5

We assume that any user running Advanced Reporter is familiar with the Internet and using a web browser. For information on the Netscape Navigator or Microsoft Internet Explorer web browsers, refer to the user documentation that came with the browser's software.

▼ To start VERITAS NetBackup Advanced Reporter 4.5:

1. Start the web browser on your computer.

2. Access the Advanced Reporter program by entering the Uniform Resource Locator (URL) in the **Location** or **Address** box and pressing [Return]. For example,

   http://<*servername*>.<*yourdomain*>:<*port*>/nbar.html (UNIX)
   http://<*servername*>.<*yourdomain*>/nbar/nbar.html (Windows)

Note This will not work if the NetBackup Administrator changed the web server port during installation. Please contact your NetBackup Administrator to verify the URL if you are having trouble connecting to VERITAS NetBackup Advanced Reporter 4.5.

We suggest you add the Advanced Reporter program URL as a **Bookmark** or **Favorite** for easy access.

As Advanced Reporter is being loaded, the Loading NBAR window appears to show how much of the application has loaded. The **Start** button will appear on the opening screen after the application has loaded.

Licensing Issues

Note If you are changing from a demo license to a permanent license you must wait for NBAR data collection to process this new information before the permanent license appears. By default, the collection is scheduled to take place at 7 a.m.

- If VERITAS NetBackup DataCenter was installed with a license key including the Advanced Reporting option, you will not be required to supply a license key during installation of NetBackup Advanced Reporter 4.5.
- If you attempt to install NetBackup Advanced Reporter 4.5 without a license key, you will be prompted to enter the license key during the installation.
- If you receive an error message that the license key is corrupted or invalid, you must re-enter the key. On UNIX systems, run the following command and enter the license key again:

  `<install_path>/netbackup/bin/admincmd/get_license_key,` where *install_path* is the directory in which NetBackup resides.

  On Windows systems, exit the NBAR installation and run the NetBackup Administration Console. From the **Help** menu select **License Keys** > **Add Keys**. Add your NBAR license key again. Right-click on the key you just added to display a Properties sheet. Make sure the **Product** field is appropriate for the type of NetBackup license you have. Verify that **Valid**: = Yes. Check the expiration date.

  On both UNIX and Windows systems, running `bpminlicense` from the command line will display license key information. Adding the `-verbose` option will display information about all keys. Adding `-nb_features -verbose` will display only information about valid NetBackup license keys. `bpminlicnese` is located in the `NetBackup\bin\admincmd` directory.

What Is the Configuration Utility?

The NBAR installation asks you to make some configuration decisions. If you want to change those settings, or others that are not addressed in the installation, NBAR provides a command-line based configuration utility, arconfig. arconfig modifies a configuration file called nbar.conf. In previous versions of NBAR, the nbar.conf file was called nbar.cnf.

The arconfig utility performs one task at a time. If you want to schedule the data loader, add a server to the GDM domain, and print out the current configuration, these must be separate procedures. You can also use this utility to report on the current configuration.

In classic NBAR configurations that only have one NBAR server, the main functions of this utility are to modify the schedule for the data loader and to change configuration settings in the nbar.conf file.

In NBAR plus GDM configurations, the main functions of this utility are to modify schedules for the data loader and the rollup process, to change configuration settings in the nbar.conf file, and to modify the list of NBAR servers under GDM control.

In both GDM and non-GDM environments you can set data collection times, set database purge times, and change the default time span for reports. The tables below specify the options for each type of server (NBAR master, NBAR managed server, and GDM master), and which ones you can modify.

To Access the Configuration Utility

This is a command line utility. From the command line of the machine on which you want to make the change, navigate to the following directory.

- On UNIX systems: `<install_directory>/bin/arconfig.sh`
- On Windows systems: `<install_directory>/bin/arconfig.bat`

For online help with the arconfig command, type -h or --help for a brief usage statement, or --man for a complete description of the options.

Modifying Configuration Information

Run the configuration utility on the command line of the server you want to modify.

The syntax for the utility is:

`arconfig` *-option [newdata]*

where

-option is the letter or phrase which specifies the action you want to perform and

newdata specifies what is acted on, or provides a new value for the specified option.

For example, if you want to join a GDM domain where the GDM server is called mango, from the command line of the NBAR server that you want to become part of the domain, you would type the following:

`arconfig -j mango`

The section below describes some actions you may want to perform using arconfig. Brackets indicate optional options.

How Do I Display Configuration Details?

There are several ways to report configuration information.

Option	Description
--print	This option lists all information from bp.conf and from the nbar database.
-g or --list	This option lists all the GDM managed servers. It will only work on a GDM server.
-c or --current	This option lists the current configuration information for all GDM managed servers from the NBAR database. It will only work on a GDM server.

How Do I Change Configuration Information Locally?

When you change configuration data on your local system, a backup configuration file is created. This file is called `nbar.conf.bak` and is located in the `/tmp` directory on UNIX systems (or in `\$TMPDIR` on HP-UX if the environment variable $TMPDIR is set) and in the `\tmp` directory on Windows systems.

If you are changing the NetBackup configuration on a UNIX NetBackup server, a backup copy of the `bp.conf` file will be created in `/tmp` (or in `\$TMPDIR` on HP-UX if the environment variable $TMPDIR is set). The backup file will be named `VERITASnbar-bp-conf.bak`.

Use the following options in combination with the keys listed in the option tables at the end of this section.

Option	Description
-b or --bpchange	This option changes the local bp.conf file by adding key/value pairs. For example, `arconfig -b SERVER=peach.xyz.com`

Option	Description
-n or --nbarchange	This option changes the local nbar.conf file by adding key/value pairs. For example, `arconfig -n growtrend1=5 -n volumepctg=10.`

How Do I Change the Database Port?

The database server requires a TCP port. The default port is 3306. The default port number is registered to MySQL with the Internet Assigned Numbers Authority (http://iana.org).We suggest you use the default port unless it is already in use. The steps below change the port referenced by the configuration utility and the data collection processes.

▼ If you need to reconfigure the database port:

1. From any server, access the command line.
2. Type `arconfig -P portnumber`,

   where port number is the new number of the database port.

▼ To reconfigure the database port for the GDM server:

1. From any server, access the command line.
2. Type `arconfig --momport <portnumber>`

   where port number is the new number of the database port for the GDM server.

How Do I Create a GDM Server?

To create a GDM server from a standalone NBAR server, use the -a switch. You must specify the same database port for both the NBAR server and the GDM server.

▼ To create a GDM server:

1. From the NBAR server, access the command line.
2. Type `arconfig -a --port <portnumber> --momport <portnumber>`

How Do I Modify a Threshold Option for a GDM Server?

The values for options such as, after how many occurrences should an error be highlighted, are initially set to a standard default. If you want to change these options, you need to modify the `nbar.conf` file on that machine.

▼ To change a threshold option:

1. From the server for which you want to make the change, access the command line.
2. Type `arconfig -n ErrorCount=<number>`

   where `<number>` is the number of occurrences of an error above which the value should be highlighted.

How Do I Delete a Server from the GDM Domain?

The list of managed servers is stored in the `netbackup/bin/bp.conf` file on UNIX and in the registry on Windows.

▼ To delete a server from the list of GDM managed servers:

You must run this command from both the GDM server and from the managed server you want to remove.

1. From each server, access the command line.
2. Type `arconfig.sh -x <servername>` on UNIX systems, or

   type `arconfig.bat -x <servername>` on Windows systems

   where <*servername*> is the name of the managed server you want to remove.

Note The -x option will delete a managed server from the NBAR configuration. You will need to remove any data collection processes that are scheduled on the managed server manually through crontab or AT.

How Do I Join a GDM Domain as a Managed Server?

You can only join an existing domain from an NBAR server.

▼ To add a server to the list of GDM managed servers:

1. From the NBAR server, access the command line.
2. Type `arconfig -j servername [-s HH.MM.SS -r HH.MM.SS -d number]`

where servername is the name of the GDM server, -s is the SORD of the managed server, -r is the time the managed server rolls up to the GDM server, and -d is the dormancy threshold for the managed server (in days).

How Do I Schedule Data Collection Processes?

By default, the NBAR installation will schedule the data loader process to run at 7:00 a.m. If you are running NBAR in a GDM environment, the installation will also schedule the rollup process to run at 7:30 a.m. If you want to change collection times or schedule the data loader to run more than once a day, you can do so using the configuration utility.

We recommend that you run data collection processes during a time of relatively little NetBackup activity. We also recommend that you run the data rollup process after the data loader. This sequence allows the data rollup to encompass as many completed jobs as possible.

Use the options in the table below to schedule data collection.

Option	Description
-L or --installloader=<time>	This option schedules a daily run time for the data loader. For example, --installloader=”8:00”
-I or --installpusher=<time>	This option schedules a daily run time for the rollup process. For example, --installpusher=”8:30”
--undoloader	This option removes the AT or crontab entry for the data loader.
--undopusher	This option removes the AT or crontab entry for the rollup process
-z or --zap	This option removes all scheduled entries for the data loader and/or the rollup process.
-f or --force	This option adds parameters or makes changes without checking for correctness or prompting during the run.

What If My Managed Servers Are in Different Time Zones?

If your servers are in different time zones, you need to think about what the most effective time to push the data to the GDM server would be. This process is most easily described by example.

The Scenario

There are three managed servers: in Boston, Minneapolis, and Los Angeles.

The local database is updated every hour on all of the servers.

The GDM server is a server in Chicago (CST zone).

The SORD is 7 am EST for the office in Boston.

The SORD is 7 am CST for the office in Minneapolis.

The SORD is 3 pm PST for the Los Angeles office.

Note CST = EST - 1, PST = EST - 3

The servers in Boston and Minneapolis have set the rollup to ‘previous day’.

The server in LA has set the rollup to ‘same day’.

Time	Actions
6 am EST Tuesday	The managed servers update the local databases in Boston, Minneapolis, and LA. The Boston and Minneapolis managed servers are collecting data that will count as *Monday’s* jobs. The Los Angeles managed server is collecting data that will count toward *Tuesday’s* jobs.
7 am EST Tuesday	The managed servers update the local databases in Boston, Minneapolis, and LA. **BostonÕs daily GDM rollup starts** The Boston managed server connects to the GDM server and updates the GDM database with the data from Monday. The server in Minneapolis is still collecting data for *Monday’s* jobs. The sever in LA is still collecting data for *Tuesday’s* jobs.
8 am EST Tuesday	The managed servers update the local databases in Boston, Minneapolis, and LA. Boston is starting to collect data for Tuesday. **MinneapolisÕ daily rollup starts** The Minneapolis managed server connects to the GDM server and updates the GDM database with the data from Monday. LA is still collecting data for Tuesday.

Time	Actions
9 am EST Tuesday, and hourly until 6 pm EST Tuesday	The managed servers update the local databases in Boston, Minneapolis, and LA.
6 pm EST Tuesday	The managed servers update the local databases in Boston, Minneapolis, and LA. **Los AngelesÕ daily rollup starts** The LA managed server connects to the GDM server and updates the GDM database with the data from Tuesday. Boston and Minneapolis are still collecting data for Tuesday.

The Results

In this scenario, the GDM server has all the data collected by the managed servers for *Monday's* NetBackup activities after 8 am EST on Tuesday. Boston's Monday rollup happened at 7 am EST, Minneapolis' Monday rollup happened at 8 am EST, and LA's Monday rollup had happened the day before at 6 pm EST.

As you can see, it is important to think through this process so that you can choose times for the rollup process to run in a way that captures most if not all of a day's backup activity and allows you to get an accurate picture of backup activity in your environment.

If possible, schedule the data rollup after the start of the reporting day (SORD), so that the rollup can capture most if not all of the previous day's information.

Command Line Options for the Configuration Utility

The options in the tables below provide a way for you to change the configuration of your managed servers. You do not have to use this utility; it is designed to make your NBAR or GDM environment as flexible, and therefore, as useful, as possible.

Options for Servers Which Are Part of a GDM Domain

nbar.conf options for GDM servers and managed servers

For Which Server	Option	Description
all servers	-p	Lists all options from both bp.conf and the NBAR database.
all servers	-c	Lists the current configuration for all NBAR managed servers.
all servers	-b	Changes the local configuration file by adding key / value pairs.
all servers	-n	Changes the local nbar.conf file by adding key / value pairs.
all servers	-m	Changes the database host for all queries. If the new database host has a different port number, add it to the server name after a colon. For example, arconfig -m peach:8081
all servers	editcrontab loader	Runs the loader at the time specified every day.
all servers	-h	Prints a usage statement for the arconfig utility options.
all servers	-f	Makes changes without checking for correctness of the changes.
all servers	-H, or --host	Indicates the name of the host machine you wish to query.
all servers	-P, or --port	Sets the port for the database
all servers	--man	Displays a detailed help for the configuration utility
all servers	-h, or --help	Displays a brief usage statement for this utility.
GDM server	-l	Lists all NBAR managed servers.
GDM server	-a	Adds a managed GDM server to the GDM domain
GDM server	-u	Updates file information on the GDM server
all servers	-x, or --xdel	Removes a managed server from a NetBackup Advanced Reporter GDM configuration. Must be run from both the GDM server and the managed server. You will still need to remove any scheduling on the local server manually.

nbar.conf options for GDM servers and managed servers

For Which Server	Option	Description
managed server	-s	Configures the SORD of the NBAR managed server. The default is 7:15 a.m.
managed server	-r	Configures the rollup time of the NBAR managed server.
managed server	-d	Configures the dormancy threshold for the data from this NBAR managed server.
managed server	-j	Adds any server to a GDM domain. **Note** Only one server may be added at a time
managed server	editcrontab pusher	Initiates a rollup at the time specified every day.

Options for GDM Servers Only

The italicized options in the table below represent options that you must configure in the order in which they appear in the nbar.conf file for each NBAR server.

Option	Description
PurgeFrequency=	This value indicates how often NBAR should delete information from its databases.
DataLife=	This value indicates how long data should remain in the database. When the data expires, it will be deleted the next time the database is purged.
ovdir=	This value is the path to the directory where NetBackup is installed for the system which also has NBAR installed. This information is picked up by NBAR from NetBackup's bpconfig file or from the Registry.
domainname=	This value indicates the domain the NBAR server resides in. This value is entered at installation and should not be changed here as it also is stored in other locations.
ErrorPctg=	If the percentage of failed jobs exceeds the percentage set by this option, the field's value is highlighted in the Global Error Details report.

Option	Description
ErrorCount=	If the number of occurrences of an error exceeds the number set by this option, the field's value is highlighted in the Global Error Details report.
GrowTrend1=	If the percentage of failed jobs exceeds the percentage set by this option, the **Growth Trend** field displays a "fast-growing" icon.
GrowTrend2=	If the percentage of failed jobs exceeds the percentage set by this option, but is less than the GrowTrend1 option, the **Growth Trend** field displays a "moderately-growing" icon.
GrowTrend3=	If the percentage of failed jobs is less than the percentage set by this option, but is more than the GrowTrend4 option, the **Growth Trend** field displays a "moderately-decreasing" icon. **Note** This value should be negative.
GrowTrend4=	If the percentage of failed jobs is less than the percentage set by this option, the **Growth Trend** field displays a "fast-decreasing" icon. **Note** This value should be negative.
VolumePctg=	If the annual percent changed of the weekly volume of data backed up is greater than the percentage set by this option, then the **Annual% Changed** field adjacent to the **Weekly Volume** field is highlighted in the *Global Backup Growth* report.
FilePctg=	If the annual percent changed of the weekly number of files backed up is greater than the percentage set by this option, then the **Annual% Changed** field adjacent to the **Files Volume** field is highlighted in the *Global Backup Growth* report.
Server=	The name of an NBAR managed server.
RollupTime= (read only)	The time that the NBAR managed server sends its data to the GDM server. This is a read-only value which the managed server updates when you run the configuration utility on the managed server.
DormantThresh=	The dormancy threshold is the number of days the *Global Media Usage* report uses to determine how many tapes are candidates for recycling. The default dormancy threshold value is 40 days. NBAR considers a tape ready for recycling if the tape is full but not expired (inactive) and the retention level for the tape is further away than the dormancy threshold.

Option	Description
SORD=	SORD stands for Start of Reporting Day. It represents the user-defined start of the GDM reporting day for this server (in time local to the server).The default value for the SORD is 7:15 a.m.
KeepLogs=	This option defines how long logs are kept. It has a default value of seven days. You can set this value on the command line, but not through the GUI.
Verbosity=	This option determines how much information NBAR logs. There are two valid values: 0 (log only essential information) and 1 (log all information). The default value is 1.

Options for GDM Managed Servers Only

The italicized options in the table below represent options that you must configure in the order in which they appear in the nbar.conf file for each NBAR server.

option	Description
PurgeFrequency=	This value indicates how often NBAR should delete information from its databases.
DataLife=	This value indicates how long data should remain in the database. When the data expires, it will be deleted the next time the database is purged.
ovdir=	This value is the path to the directory where NetBackup is installed for the system which also has NBAR installed. This information is picked up by NBAR from NetBackup's bpconfig file or from the Registry.
domainname=	This value indicates the domain the managed server resides in. This value is entered at installation and should not be changed here as it also is stored in other locations.
GDM serverServer=	This option indicates to which GDM server the managed server should roll up its data.
RollupTime=	This option sets the time the managed server should send its data to the GDM server.

option	Description
KeepLogs=	This option defines how long logs are kept. It has a default value of seven days. You can set this value on the command line, but not through the GUI.
Verbosity=	This option determines how much information NBAR logs. There are two valid values: 0 (log only essential information) and 1 (log all information). The default value is 1.

Options for Non-GDM NBAR Servers

For NBAR servers which are not part of a GDM environment, use the configuration utility to set data loader options, set the schedule for the data loader, and set other options in the nbar.conf file, such as database purge frequency.

Refer to the table below for a list of all options you can set in the nbar.conf file.

nbar.conf settings for NBAR servers

option	Description
PurgeFrequency=	This value indicates how often NBAR should delete information from its databases.
DataLife=	This value indicates how long data should remain in the database. When the data expires, it will be deleted the next time the database is purged.
ovdir=	This value is the path to the directory where NetBackup is installed for the system which also has NBAR installed. This information is picked up by NBAR from NetBackup's bpconfig file or from the Registry.
domainname=	This value indicates the domain the NBAR server resides in. This value is entered at installation and should not be changed here as it also is stored in other locations.
KeepLogs=	This option defines how long logs are kept. It has a default value of seven days. You can set this value on the command line, but not through the GUI.
Verbosity=	This option determines how much information NBAR logs. There are two valid values: 0 (log only essential information) and 1 (log all information). The default value is 1.

Backing Up the NBAR Database

We recommend you back up the NBAR database on a regular basis.

❖ To backup the NBAR database:

In NetBackup, create a policy to back up the files in `/opt/VRTSnbaro/var` for UNIX systems, or `c:\Program Files\VERITAS\NetBackup Advanced Reporter\data` for Windows systems.

The directory paths in these examples use the default directory configuration. If you change the location of the NBAR directory during installation, the paths will be different on your system.

Note Be sure to schedule the backup during a time NBAR's data collection processes are not running.

Troubleshooting NBAR 11

This chapter explains some utilities provided to help you troubleshoot your NBAR installation, and describes some known issues and solutions in NetBackup Advanced Reporter 4.5.

This chapter contains information on the:

- Logging Utilities
- Database Export Utility
- Known Issues

How the Logging Utilities Work

NBAR 4.5 provides several error logging utilities. While you can access these logs, and they may provide you with useful information, the information is collected to help our support engineers, and is therefore somewhat cryptic. We suggest you use the *NetBackup Troubleshooting Guide* and the topics listed in this chapter as your first reference, before turning to these log files.

Location of Logs

NBAR logs messages to one or more places, depending on the nature of the message and the verbosity level setting (see the section below on verbosity levels).

- MySQL nbarlog table

  Messages will be logged to this table if they meet verbosity guidelines. Error messages will always be logged to this table.

- If you create a directory called the same thing as the data loader process (arloader) or the data rollup process (arpusher), in the same directory as the other NetBackup logs, NBAR will write messages to these log files. Use these logs to investigate problems with the data collection processes.

For example, if you want to create a log file of messages generated by the data loader on a Solaris system, you would create a directory named arloader under the /usr/openv/netbackup/logs.

A log file is generated each time the data collection process runs. The logs are text files named with the date created. For example, log.081301 is a log file created on August 13, 2001

- Serious NBAR errors, such as a database malfunction, will be written to the system log on UNIX systems, or the event log on Windows systems.

Logging Configuration

There are three ways you can modify how NBAR handles logging. These are the retention period for the nbarlog table entries, the level of messages that are logged (see Verbosity Levels), and whether or not messages are written to the nbarlog table. A parameter in the nbar.conf file controls each of these values.

nbar.conf logging parameters

Parameter	Description
KeepLogs	The number of days to save nbarlog table entries. Default value is seven days.
Verbosity	The level of messages to be logged. See Verbosity Levels below.
NoTableLogs	Turns off logging to the nbarlog table (errors will still be logged.

Verbosity Levels

For an message to be logged, the verbosity level of the message must be equal to or greater than the verbosity level set in the nbar.conf parameter. The default verbosity level is 2 (all messages will be logged).

Description	Severity	Verbosity
Support/Engineering Messages Only	2	2
Customer Information	4	1
Customer Warnings	8	1

Description	Severity	Verbosity
Customer Errors	16	0 (these errors will always be logged)

Log File Purging

The log files that reside in the NetBackup Logs directory are purged by the same mechanism that purges other NetBackup log files. The amount of time these log file s are kept is defined in NetBackup System Configuration, Global Attributes, Duration to Retain Logs. See the NetBackup *System Administrator's Guide* for more information.

The nbarlog table entries are purged based on the value of the KeepLogs parameter in the nbar.conf file.

Logging Utilities

Below is a description of the ardumplog and the parameters you can use to get information from the log files.

ardumplog

ardumplog is a command line utility that displays the contents of the database for a period of time you define. Use ardumplog to investigate data loader failure or to send diagnostic information to VERITAS support. The parameters for this utility are listed below.

Parameter	Description	Format/Example
-v or --verbose	This parameter prints out all the details for the logged information.	N / A
-s or --startime	The beginning of the time period of the logged information you want to display. Defaults to three days before current date. Uses 24-hour time.	YYYY-MM-DD hh:mm:ss For example, 2001-SE-02 11:14:32 would be September 2, 2001, at 11:14 a.m.

Parameter	Description	Format/Example
-e or --endtime	The end of the time period of the logged information you want to display. Defaults to the current date. Uses 24-hour time.	YYYY-MM-DD hh:mm:ss For example, 2001-SE-05 13:32:54 would be September 5 2001, at 1:32 p.m.
-d or --dbhost	The name of the server which contains the NBAR database. This value defaults to the local machine. The port number is optional.	servername [:portnumber] For example, hancock.veritas.com:3306
-h or --help	This parameter displays a list of possible parameters.	N / A

What Is the Database Export Utility?

The database export utility, **nbardbex**, is a command-line utility that allows you to select a list of records from the VERITAS NetBackup Advanced Reporter 4.5 database and export them to a file or another application. This feature may be particularly useful if you want to use a spreadsheet program such as Excel to analyze the information pulled from the database.

Using the Database Export Utility

Type the name of the utility on the command line, and use the parameters listed below to determine which database and which records the utility selects.

The name of the utility is **nbardbex**. Required parameters are server, **-S**, and duration, either **-s** and **-e**, or **-hoursago**. If you do not specify a time, the database export utility assumes midnight (0:00) on the date indicated. Use **-H** to place headings on the data columns, and **-d** to change the default data delimiter. To export data from a server running on a nondefault port, include the port number in the command.

For example:

```
nbardbex -S peach:6606 -hourago 48
```

where 6606 is the nondefault port number.

Sample Output

```
533 0    B    Complete 0 "2001-12-07 21:51:39" 0   txb-test  Differential-Inc
peach.min.ov.com peach.min.ov.com  0 Backup 100 peach-dlt2-robot-tld-0"" '/var/adm'
534 0    B    Complete 0 "2001-12-07 22:01:38" 0   txb-test  Full
peach.min.ov.com peach.min.ov.com 0 Backup 100 peach-dlt2-robot-tld-0" "'/var/adm'
```

Parameters

-S The name of the master server on which the NBAR database resides

-s The date and time you want to start collecting records, in the format mm/dd/[yy]yy [hh:ii]. (The brackets indicate optional information.)

-e The date and time you want to finish collecting records, in the format mm/dd/[yy]yy [hh:ii]. (The brackets indicate optional information.)

-hoursago Number of elapsed hours counting backward from the current time from which to collect records. For example, if it is now noon, and you choose 15 as the value for the -hoursago parameter, the database export utility will collect records from the previous 15 hours, that is, since 9 p.m. the previous evening.

-H This parameter places column headings in the output

-d The character you place after this parameter will act as the field delimiter. Space or blank is not an acceptable delimiter. A tab is the default delimiter.

Note You must use **-s** and **-e** together. **-s** and **-e** and **-hoursago** are mutually exclusive.

Example

nbardbex -S servername -s 11/01/2001 -e 11/02/2001

This example would give you information on all NetBackup jobs beginning at midnight, November 01, 2001, and ending at midnight, November 2, 2001.

Record Values

Most records represent a complete job run by NetBackup. However, the database export utility will generate a record for each file system or directory specified in the NetBackup policy. Therefore, the utility will create more than one record for jobs that back up or restore more than one file system or directory.

Each record contains the information outlined below. Use the -H parameter if you want the headings to appear on the data you choose to output.

Heading	Description
Job ID	The ID number of the job.
Job PID	Always 0.
Type	The type of job. These are standard NetBackup job designations.
State	Always ‘Complete’.
Status	Indicates the success or failure of the job. These are standard NetBackup job completion codes.
Start Time	The time the job started.
End Time	The time the job ended.
Elapsed Time	The amount of time the job took.
Kilobytes	The number of kilobytes transferred during the job.
# of Files	The number of files transferred during the job.
KB Per Second	The number of kilobytes transferred per second during the job.
Policy	The policy name of the job.
Schedule	The name of the schedule within the policy.
Client	The name of the machine from which data was backed up.
Media Server	The name of the media server the data was backed up to.
Attempt	Always 0.

Operation	Backup or Restore only.
% Comp. (estimated)	Always 100.
Storage Unit	The name of the storage unit the data was backed up to.
Owner	Always ‘’.
File List	The file system or directory selected by the backup policy. If more than one file system is selected, NBAR will create a record for each file system or directory. For example, c:\dir1 d:\dir2. This information is not available for multi-stream clients or clients with a local include/exclude list.
Media ID	The ID of the media on which the information was backed up (tape_barcode1, tape_barcode2).
Tape_Drive	The ID of the tape drive that was used when the information was backed up.

Troubleshooting the Database Export Utility

Errors with the database export utility have one of two causes: either there is a a problem accessing the database, or there is mistake on the command line.

Database Error

If the facility part of the error message says “mysql client” or “mysql server”, than the problem is with the database. In that case, please note the error code (at the end of the first line), and the name of the MySQL API (on the second line), and contact Customer Support.

If you cannot connect to the database, either the database is not running, or the TCP port the client (the machine running the applet) is using to connect to the database is incorrect.

Command Line Error

If the error is on the command line, the facility will be “nbar unknown” or “nbar command”. In that case, the following information may help:

Error codes contain two lines. The first identifies the problem, and the second line provides additional information.

The first line consists of the following:

severity: (value) facility: (value) code: (value)

Values for the first line are as follows:

- Possible severity values are “informational”, “warning” and “error”.
- Possible facility values are:

  “nbar unknown” - something in the export utility code other than command-line interpretation

  “nbar command” - export utility command-line interpretation

  “mysql client” - MySQL code incorporated into the export utility

  “mysql server” - MySQL server failures
- Possible code values depend on the context and consist of a brief description of the problem.

Example

Where the server name is server1:

```
server1% nbardbex -S server1 -hoursago 168 -s 11/13/2001

severity: error  facility: nbar command  code: invalid option
combination

operand value is "11/13/2001"
```

This error tells you that **`-hoursago`** and **`-s`** options are incompatible and that the value of the option in which the error was detected was that for the start date.

Licensing Issues

Note If you are changing from a demo license to a permanent license you must wait for NBAR data collection to process this new information before the permanent license appears. By default, the collection is scheduled to take place at 7 a.m.

- If VERITAS NetBackup 3.4 DataCenter was installed with a license key including the Advanced Reporting option, you will not be required to supply a license key during installation of NetBackup Advanced Reporter 4.5.
- If you attempt to install NetBackup Advanced Reporter 4.5 without a license key, you will be prompted to enter the license key during the installation.

- If you receive an error message that the license key is corrupted or invalid, you must re-enter the key. On UNIX systems, run the following command and enter the license key again:

  `<install_path>/netbackup/bin/admincmd/get_license_key,` where *install_path* is the directory in which NetBackup resides.

  On Windows systems, exit the NBAR installation and run the NetBackup Administration Console. From the **Help** menu select **License Keys** > **Add Keys**. Add your NBAR license key again. Right-click on the key you just added to display a Properties sheet. Make sure the **Product** field is appropriate for the type of NetBackup license you have. Verify that **Valid**: = Yes. Check the expiration date.

  On both UNIX and Windows systems, running bpminlicense from the command line will display license key information. Adding the `-verbose` option will display information about all keys. Adding `-nb_features -verbose` will display only information about valid NetBackup license keys. `bpminlicnese` is located in the `NetBackup\bin\admincmd` directory.

Starting the httpd and database daemons - UNIX only

If you did not choose to have the daemons restarted automatically after a system reboot, you must start them manually.

▼ **To start the daemons:**

1. Change to the following directory:

   On Solaris systems: `/etc/init.d/nbar`

   On HP-UX systems: `/sbin/init.d/nbar`

2. From this location, type `start` to run the daemons or `stop` to halt them.

Starting the Applet

Need to Upgrade the Microsoft Virtual Machine in IE

If the NBAR GUI has display problems such as too-small toolbar buttons, reports not displaying on screen, or a persistent hourglass, you may need to update your version of the Microsoft virtual machine (VM). Download and install the latest version of the Microsoft VM from `http://www.microsoft.com/java.`

Microsoft Internet Explorer 5.5

There are several situations in which the Start button may not appear on the NBAR splash screen.

- The Advanced Reporter Java applet is distributed to a Microsoft Internet Explorer 5.5 web browser as a Java distribution unit. Java distribution units need lots of disk space on Windows NT machines configured with FAT file systems. Specifically, the drive containing the directory where temporary internet files reside (usually the same drive where Windows NT is installed) must have at least 100 MB of free disk space available when you download the Java applet for the first time. If you try to download and run the applet on a system with insufficient disk space, the **Start** button may not appear on the Advanced Reporter splash screen.

  For further details, refer to the following Microsoft Knowledge Base article:
  http://support.microsoft.com/support/kb/articles/q232/6/38.asp

- Occasionally, and particularly after an upgrade, the *.jar file for the applet must be manually removed to force an upgrade of the application. The procedure for removing the file is slightly different for each browser and operating system.

Netscape 6

- Only a preview release of Netscape 6 was available for testing. On some platforms, the JRE is not installed automatically with Netscape 6. Before running NBAR for the first time, make sure that Java support is enabled, and that the JRE is installed and accessible. To verify that the Java plugin is installed, enter “about:plugins” as a URL. You should see Java Plugin in the list of installed plugins.

  The first time you access the Java applet, it is downloaded and stored on your hard disk. This requires write permission to the download directory. If you do not have write access to the directory, the installation of NBAR will fail. The dialog indicating the failure will show the path for the download directory. Enable write permissions to this directory and access NBAR again.

Allowing NBAR Access to GDM Data

Your NetBackup GDM configuration must be up and running for NBAR to access information from the managed servers. This means the GDM server must ‘know’ about all the managed servers through an entry in the bp.conf file. Follow the instructions below to add these entries.

For more information about NetBackup GDM configuration, refer to the NetBackup 4.5 *System Administrator’s Guide*.

▼ To configure UNIX servers:

1. On each UNIX Netbackup master server, add a MASTER_OF_MASTERS entry for the GDM server to the `bp.conf` file.

2. On each UNIX NetBackup master or media server, add a SERVER entry for the GDM server to the bp.conf file.

   For a GDM server called owl, your entries would look like this:

   ```
   MASTER_OF_MASTERS = owl
   ```

   ```
   SERVER = owl
   ```

3. On a master server, stoop and restart the NetBackup `bpdbm` daemon after adding the `bp.conf` entries.

▼ To configure Windows servers:

1. On each master server, specify the GDM server.

   a. In the NetBackup Administration window, from the **Start** menu, click **NetBackup Configuration**.

      The Configure - NetBackup window displays.

   b. Select the NetBackup master server, and from the **File** menu choose **Properties (Read/Write)**.

      The Master Server Properties dialog box displays.

   c. On the **GDM** tab, find the column for the master server you want to add to the GDM configuration and add the name of the GDM server to the **Global Data Managers** section.

2. On both master and media servers, add the GDM server to the server list.

   a. In the NetBackup Administration window, from the **Start** menu, click **NetBackup Configuration**.

      The Configure - NetBackup window displays.

   b. Select the NetBackup master server, and from the **File** menu choose **Properties (Read/Write)**.

      The Master Server Properties or Media Server Properties dialog box displays.

c. On the **Servers** tab, find the column for the server you want to add to the GDM configuration and add the name of the GDM server to the **Additional Servers** section.

Persistence of GDM Tree in Console after Uninstalling

If you have configured a server as a GDM server, then uninstall NBAR from the server, and reinstall NBAR on that machine, but configured as a standalone server, the GDM tree may still be visible on the left side of the NBAR Java Console.

If this occurs, from `<install_directory>/bin run` the following command:

On UNIX: `arconfig.sh -xdel <server_name>`

where `<server_name>` is the name of the server you are trying to reconfigure.

`On Windows: arconfig.bat -xdel <server_name>`

where `<server_name>` is the name of the server you are trying to reconfigure.

Note We continue to retain this GDM information as a precaution in case incorrect options were chosen when the product was installed.

Database Issues

The known issues in this section involve database tables or connection problems.

Hosts Table

The hosts table contains information about each machine known to Advanced Reporter. A host will persist in the hosts table as long as it has job information associated with it, even if the host has been removed from all policies.

If the host does not have job information associated with it, it will be deleted from the database only when the value set for the purge frequency of the database is reached. The database is purged weekly by default.

Unable to Connect to Database Error Message

If you receive this message, it means the client (the machine running the applet) could not connect to the database server. The database may not be running, or the TCP port the client is using to connect to the database may be incorrect. Follow the instructions below to check these possibilities on Windows or UNIX systems.

Windows NT

- To verify that the database server is running, from **Control Panel\Services** check the status of the NetBackup Advanced Reporter Database Server and System Monitor.

- To check the port number of the client, navigate to the directory where NBAR is installed. From the htdocs directory, open nbar.html. Search for 'serviceport' to find the value of the port number for the client.

  To find the value of the port number for the database server, navigate to the install directory and cd to the bin directory.

  Type `ardbd --help`

  If the database server is running, this command will list the attributes of this service. The default port number is 3306.

Windows 2000

- To verify that the database server is running, from **Control Panel\Administrative Tools\Services** check the status of the NetBackup Advanced Reporter Database Server and System Monitor.

- To check the port number of the client, navigate to the directory where NBAR is installed. From the htdocs directory, open nbar.html. Search for 'serviceport' to find the value of the port number for the client.

  The database (ardbd) uses the port in `c:\WINNT\ardbd.ini`. In NBAR 4.5, the port number is also saved in the `nbar.conf` file as *mysqlportlocal*. Or, navigate to the install directory and cd to the bin directory.

  Type `ardbd --help`

  If the database server is running, this command will list the attributes of this service. The default port number is 3306.

Solaris

On UNIX systems, there are several ways to check the operation of the database server.

- Typing the command

  ```
  ps -ef | grep ardbd
  ```

  should show the process ardbd running. If the database server is not running, type the command

  ```
  /etc/init.d/nbar start
  ```


to start the database.

- The UNIX socket that the process ardbd uses must be available. The default location of this file is in `/opt/SUNWnbaro/bin/.ardbd.sock`. If this file does not exist, you must reinstall NBAR.
- Check that the port number the client is using to connect to the database is the same as the one on the database server. To find the port number for the database server, type **-ef | grep ardbd**

  To find the port number for the client, cd to `/opt/SUNWnbaro/htdocs/nbar.html`.

  Type **grep serviceport nbar.html**

  to find the port number. If it does not match the database server port, you can edit nbar.html to change the value to match that of the database server's port.
- The process file `/opt/SUNWnbaro/var/<hostname>.pid` should only exist if the database server is up and running. The port number is also saved in `nbar.conf` as *mysqlportlocal*.
- Check the log file for error messages. This file can be found in `/opt/SUNWnbaro/var/<hostname>.log`. For more information about logging in NBAR, please see the "How the Logging Utilities Work" section in this chapter.

HP-UX

On UNIX systems, there are several ways to check the operation of the database server.

- Typing the command

  ```
  ps -ef | grep ardbd
  ```

  should show the process ardbd running. If the database server is not running, type the command

  ```
  /sbin/init.d/nbar start
  ```

  to start the database.
- The UNIX socket that the process ardbd uses must be available. The default location of this file is in `/usr/openv/nbar/bin/.ardbd.sock`. If this file does not exist, you must reinstall NBAR.
- Check that the port number the client is using to connect to the database is the same as the one on the database server. To find the port number for the database server, type **-ef | grep ardbd**

  To find the port number for the client, cd to `/usr/openv/nbar/htdocs/nbar.html`.

Type **grep serviceport nbar.html**

to find the port number. If it does not match the database server port, you can edit nbar.html to change the value to match that of the database server's port.

- The process file `/usr/openv/var/<hostname>.pid` should only exist if the database server is up and running. The port number is also saved in `nbar.conf` as *mysqlportlocal*.
- Check the log file for error messages. This file can be found in `/usr/openv/var/<hostname>.log`. For more information about logging in NBAR, please see the "How the Logging Utilities Work" section in this chapter.

Report Issues

This section of the troubleshooting chapter describes issues with report information.

Active Media Report

NBAR reports frozen media as a subset of active media. NetBackup does not consider frozen media to be active.

This discrepancy will be addressed in the next release of Advanced Reporter.

NetBackup Database Extension Backups in NBAR

Database backups are not reported in a consistent fashion in the Advanced Reporter reports. The following database extensions are not tracked by NBAR:

Oracle Obackup, Informix OnBar, Sybase, DataTools SQL BackTrack, Microsoft SQL Server, SAP, DB2, and Extensible Client.

Trouble Printing Reports

If you are having trouble with reports that print without graphics, or are not complete, make sure that you have downloaded and installed the latest drivers for your printer from the printer vendor.

Job Retry Information

The way NBAR and the way NetBackup record job retries is somewhat different. This can lead to discrepant reported results. We list several common situations below.

Several Status Codes, Same Job ID

If a job fails, and the same instance of the scheduler (bpsched) is still running, the scheduler will try to start the job again with the same job ID. If the job succeeds on this second try, NBAR's data loader will record the job as successful as long as the retries take place within the same instance of the scheduler. However, if the scheduler has stopped and started again, then the same job will be assigned a new job ID and NBAR will treat it as a new job.

Discrepancies with Activity Monitor

At times the number of jobs reported by My Activity Monitor will not match the number of jobs reported by NBAR. This is because the Activity Monitor records all instances of an activity -- for example, a job try that failed is recorded just as a job try that succeeded is recorded. On the other hand, NBAR is interested in the outcome of the activity -- and will record only one instance of the job if the job succeeds, no matter how many tries it took, as long as the retries take place within the same instance of the scheduler.

Activity Monitor looks only for jobs that are retried within the same instance of the scheduler, whereas the NBAR reports look to see if a job has been successful.

By default the scheduler is restarted every ten minutes, but some really big sites keep the scheduler running all the time, if they have a full schedule. This potentially creates a confusing report with lots of retries.

Upgrading to NBAR 4.5 from NBAR 3.2.1

We recommend that you be careful when you interpret data that encompasses the time period when you moved from NBAR 3.2.1 to NBAR 4.5. In NBAR 3.4 we made several changes to the way NBAR handles data to make it more consistent with the way NetBackup handles data.

Specifically, we changed the way we handled retries, we did not deal with job streams in the past, and we did not use the actual job ID in previous versions of NBAR. In NBAR 3.4 and 4.5, only one instance of a job is recorded if the job succeeds, no matter how many retries were needed. NBAR 3.4 and NBAR 4.5 handle multistreaming jobs, and uses the same job ID as NetBackup for each job.

There is no way to make data collected before you upgrade entirely consistent with data collected after the 4.5 installation. This is why we note that data reported on around the time of the transition to NBAR 4.5 may contain small inconsistencies. The alternative is to perform a clean installation and not keep any data collected by a prior version of NBAR in the NBAR database.

Database Schema for NBAR A

This appendix describes the database schema for the NetBackup Advanced Reporter database. Its purpose is to allow experienced NBAR users to develop their own NetBackup queries, and to help them understand where the data is coming from in the existing NBAR reports.

This document is intended for the technically sophisticated Netbackup Advanced Reporter user. It assumes a reasonable familiarity with both NetBackup and NBAR. Refer to existing NetBackup documentation for more information about the NetBackup databases and commands.

Note Be aware that future versions of this database will have schema changes and may be incompatible with the current schema.

Requirements

- The NBAR database uses a MySQL 3.32.37 database engine. Access to the database is through the MySQL Perl DBI.
- You must create a user name and password to use the Perl DBI interface.
- You must run the Perl DBI as a user other than root on UNIX systems, or administrator on Windows systems. This precaution is to prevent unprivileged MySQL users from gaining unauthorized access to the system.

NBAR's Application Control Schema

The application control schema consists of tables which contain data used to control the content and actions of the Reports submenu and the selected report display properties of NBAR's client browser.

Report (sub)menu information defines the tree structure of the reports menu, the display text, and the Java class file to be invoked when a menu item is selected.

All report menu information is keyed by a username column. In the current implementation, this column is always set to contain the value 'target', and provides a default implementaiton.In future releases this may contain actual user names, thereby providing automatic support for user-specific menu structures.

Report property information is keyed by the Java class name of the class which implements the report. This construction supports the dynamic inclusion or exclusion of reports in the browser and permits adjustments to the report display.

There are several Perl scripts in the `/bin/goodies` directory. Each script is written to provide the information in an existing NBAR report. These scripts are meant as examples to demonstrate the type of information you can draw from the NBAR database.

List of Database Tables

NBAR Database Tables

This section of the appendix contains a detailed description for each table that is part of the NBAR database. Tables are divided by table name.

properties

The properties table contains user-specific, dynamically specified application properties which may be read during application startup and used to customize the user's view of the application and its functionality.

properties table

Column Name	Type	Null	Key	Default	Description
username	char(12)		PRI		The name of the user these properties belong to.
property	char(40)		PRI		The name of the property.
type	tinyint(4)	Yes			0:text, 1:color, 2:font
value	char(40)	Yes			The value of the named property.

The *type* attribute is used to identify the method the application should use to parse the property value. The parsing rules for the *value* attribute are:

Property Type	Key	Formatting Rules
text	0	Any arbitrary alphanumeric string
color	1	An integer RGB color value
font	2	A comma-separated string of the format "fontFamily,fontStyle,fontSize". See java.awt.Font for more details.

catalog_index

The catalog_index table describes the actions to be made available to the end user, and the organization of these actions in the application's report browser and report menu.

catalog_index table

Column Name	Type	Null	Key	Default	Description
username	char(12)		PRI		The name of the user this catalog is displayed for.
seq	int(11)		PRI	0	The order in which to display the items.
item	char(80)				The definition of an item.
type	tinyint(4)			0	0:(sub)menu item, 1:leaf node
classname	char(50)	Yes			The class to instantiate and execute when the item is selected.

The *item* attribute is used to describe the catalog item, its place in the catalog hierarchy, and the textual description to be displayed. The parsing rules for the item attribute are recursive and in the format:

root.[submenu.[...]]leaf:

For example, to describe an item which is in the Full Backups submenu of the Management root menu, the string would look like this:

Management.Full Backups.Report Name

reports

The reports table remains in the schema for historical reasons and will be deprecated and removed from active use in release 4.5.

reports table

Column Name	Type	Null	Key	Default	Description
classname	char(50)		PRI		The Java class name of the class which instantiates the report.

reports table

Column Name	Type	Null	Key	Default	Description
description	char(60)	Yes			The textual description of the report.
type	tinyint(4)	Yes			Deprecated.

report_properties

The report properties table describes the dynamically adjustable properties of each report in the catalog_index table. These properties are correlated by user, so that each individual user may customize the 'look-and-feel' of the reports...

report_properties table

Column Name	Type	Null	Key	Default	Description
classname	char(50)		PRI		The fully-qualified Java class name of the report with which the property is associated.
username	char(12)		PRI		The user to whom the property is assigned.
property	char(40)				The name of the property.
type	tinyint(4)			0	
value	char(40)				The value of the property.

hosts

The hosts table contains information about each host known to VERITAS NetBackup Advanced Reporter. This table consolidates information about all the hosts found by the data parser when it parses the NetBackup class definitions.

hosts table

Column Name	Type	Null	Key	Default	Description
hostname	char(40)		PRI		The simple host name.

hosts table

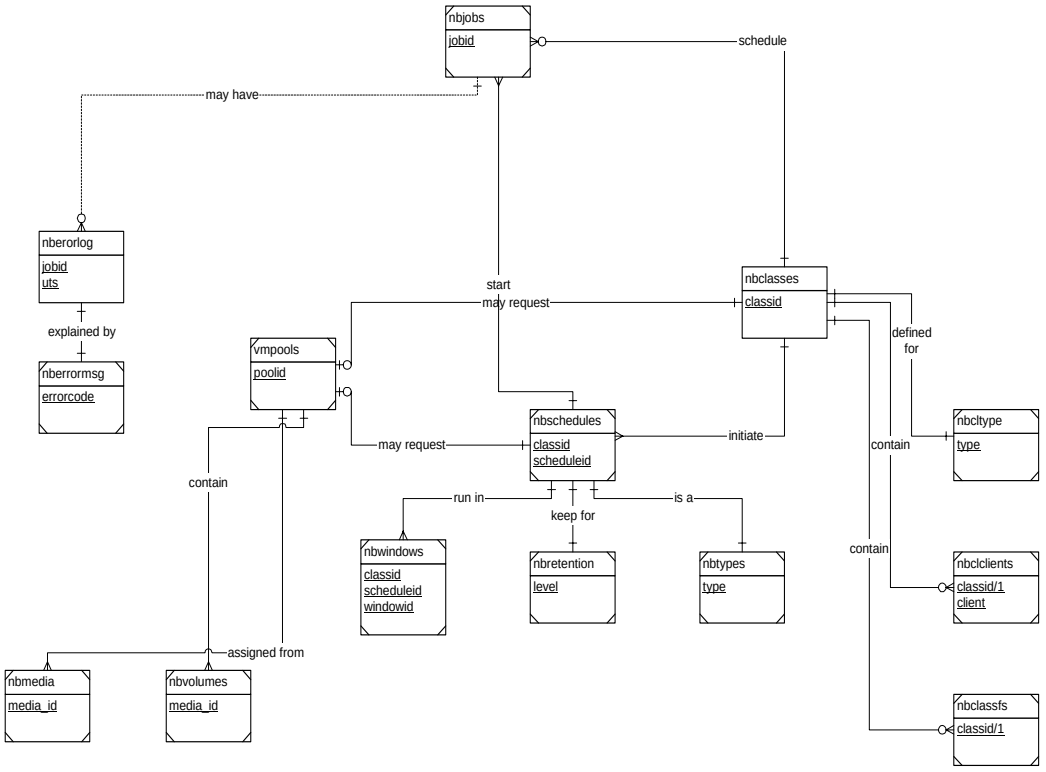
Column Name	Type	Null	Key	Default	Description
domainname	char(60)	Yes			The name of the domain the host resides in. NULL if unknown.
ipaddr	char(16)	Yes			The IP address of the host.
role	int(11)	Yes			0: Master, 1: Media, 2: Client
type	char(80)	Yes			The hardware platform, taken from the client information in the NetBackup class definition.
organization	char(80)	Yes			Unused.
description	char(80	Yes			Unused.
location	char(80	Yes			Unused.
spare1	char(80	Yes			The client operating system, taken from the client information in the NetBackup class definition.
spare2	char(80	Yes			Unused.
spare3	char(80	Yes			Unused.
spare4	char(80	Yes			Unused.
spare5	char(80	Yes			Unused.
spare6	char(80	Yes			Unused.

NetBackup Database Schema

This section of the appendix describes the tables found in NetBackup's database.

Entity Relationships

Here is a diagram of the relationships between database tables in NetBackup.



NetBackup Table Definitions

This section describes the fields in each NetBackup database table.

nbjobs

Contains one row for each NetBackup job. The data contained in this table is gathered from the NetBackup Job information provided by the `bpimagelist` binary provided with NetBackup. It is further supplemented with data culled from the error log which is extracted using the NetBackup binary `bperror`.

nbjobs table

Column Name	Type	Null	Key	Default	Description
jobid	int(11)		PRI	.	The NBU job identifier. It is used to relate NetBackup jobs to entries in the nberrorlog table.
jobtime	datetime		MUL	0000-00-00	The start UTS of the job translated to DB date format.
type	char(1)		MUL		B: backup, R: restore
status	int(11)		MUL	0	-1: error occurred, refer to nberrorlog for NBU error code, 0: Successful job 1: Partially successful job
servername	varchar(255)		MUL		The name of the media server which executed the job.
clientname	varchar(255)		MUL		The name of the client the job was run on.
startuts	int(10)unsigned		MUL	0	the start UTS of the job.
duration	int(10)unsigned	YES			The time, in seconds, the job took to complete.

nbjobs table

classid	smallint(6)	YES	MUL	0	The class identifier of the NetBackup Class the job ran in. Refers to classid column in nbclasses table. –1 or NULL means unknown.
scheduleid	smallint(6)	YES	MUL	0	The schedule identifier of the NetBackup Class-Schedule the job ran in. Refers to scheduleid column in nbschedules table. –1 or NULL means unknown.
windowid	tinyint(4)	YES		0	The window the job ran in. Digit from 0-6. 0 is Sunday. 10 or NULL means unknown.
windowdate	date	YES	MUL	0000-00-00	Deprecated.
volume	int(10)unsigned	YES			The amount of data, in Kbytes, the job processed.
throughput	smallint(6)	YES			The average throughput, in Kbytes / second, the job achieved.
nfiles	mediumint(9)	YES		0	The number of files the job processed.
driveindex	tinyint(3)unsigned	YES			The index of the drive used for the job. **Note** Sometimes this field will be null for restore jobs because they do not consistently store this information.

nbjobs table

poolid	smallint(6)	YES	MUL	0	The pool identifier of the Volume Pool the media was selected from. Relates to poolid in the vmpools table. –1 or NULL means unknown.
expiry	datetime	YES			The backup image expiry date.
media_id	varchar(6)	YES			The media ID of the media the image was written to. Relates to the media ID in both the nbmedia and nbvolumes tables.
stu	varchar(128)	YES			The name of the Storage Unit used by the job. Relates to the label column in the nbstu table.
streamid	int	YES	MUL		Primary job ID for a multistream job
num_retries	int	NO		0	Tally of “adding job to queue” messages
backup_id	varchar(255)	YES			Unique ID / link to image

nberrorlog

The nberrorlog table contains one row for each “EXIT STATUS” error (errors>1) reported by NetBackup. The data contained in this table is gathered from the NetBackup error log using the `bperror` binary provided with NetBackup.

nberrorlog

Column Name	Type	Null	Key	Default	Description
jobid	int(11)		PRI	0	The identifier of the job which incurred the error. Relates to nbjobs.jobid.

nberrorlog

Column Name	Type	Null	Key	Default	Description
uts	datetime		PRI	0	The data and time the error occurred.
status	smallint(6)	YES			The NetBackup error code. Relates to nberrormsg.errorcode.

nberrormsg

The nberrormsg table is a lookup table which contains textual information about each NetBackup error code. Its contents are loaded from the NetBackup Trouble Shooting Guide...

nberrormsg

Column Name	Type	Null	Key	Default	Description
errorcode	smallint(6)		PRI	0	The NetBackup error code.
description	varchar(255)				A short description of the error.
explanation	blob	YES			A detailed description of the error.
recommendation	blob	YES			The recommended trouble shooting actions.

nbclasses

The nbclasses table contains NetBackup class definitions. The data contained in this table are gathered from the NetBackup class definitions using the bpcllist binary provided with NetBackup.

Both current and past class definitions are recorded in this table. During the data load process, each current class definition is compared with its copy in the database. If a discrepancy is found the existing row is marked as retired and new information is inserted.

nbclasses table

Column Name	Type	Null	Key	Default	Description
classid	smalliint(6)		PRI	auto inc.	The classid is an artificially generated key which provides a unique identifier.
classname	varchar(128)				The name NetBackup gives to the class.
active	tinyint(4)			0	-1:retired, 0:active, 1:inactive in NetBackup
type	tinyint(4)			0	The backup tape. It relates to the type column in the nbtypes table.
created	date			0000-00-00	The date the row was first inserted into the table.
retired	date	YES			The date the class information was superseded by a newer definition.
compressed	tinyint(4)	N		0	Answers the question, does this class perform data compression? 0: false, 1: true
priority	tinyint(4)	N		0	Indicates the job priority. 0 = the default priority.
crossmntpts	tinyint(4)	N		0	Answers the question, should the job cross file-system mount points?
Followfs	tinyint(4)	N		0	

nbclasses table

Column Name	Type	Null	Key	Default	Description
Trueimage	tinyint(4)	N		0	Answers the question: perform true image backups? 0:No, 1:Yes
Multistream	tinyint	N		0	1: multiple streams
Maxjobs	int	N		0	The maximum number of jobs that can be started at one time. (2147483647 indicates no maximum.)
poolid	smallint(6)	YES			The default media pool for this class. (-1 or NULL if unknown.)
stu	varchar(128)	YES			The name of the associated storage unit (see nbstu).

nbclassfs

The nbclassfs table contains a list of file systems to be backed up for each class defined in the nbclasses table...

nbclassfs table

Column Name	Type	Null	Key	Default	Description
classid	smallint(6)		PRI	0	This is the class identifier. It relates to the classid column in the nbclasses table.
action	tinyint(4)			0	Reserved.
filesystem	varchar(255)		PRI		This is the name of the file system.

nbclients

The nbclients table contains a list of NetBackup clients and information about the backup jobs for those clients.

nbclients table

Column Name	Type	Null	Key	Default	Description
classid	smallint(6)		PRI	0	This is the link to the nbclasses table.
clientname	varchar(255)		PRI		This is the name of the client.
last_full_success_date	datetime				This is the date and time of the last full backup with status 0.
last_full_partial_date	datetime				This is the date and time of the last full backup with status 1.
last_full_failure_date	datetime				This is the date and time of the last full backup with an error status.
last_full_expires_date	datetime				This is the latest expiration date of a full backup with status 0.
last_incr_success_date	datetime				This is the date and time of the last incremental backup with status 0.
last_incr_partial_date	datetime				This is the date and time of the last incremental backup with status 1.
last_incr_failure_date	datetime				This is the date and time of the last incremental backup with error status.
last_incr_expires_date	datetime				This is the latest expiration date of an incremental backup with status 0.

nbclients table

Column Name	Type	Null	Key	Default	Description
stream_failure_count	int				

nbcltypes

The nbcltypes table contains a description of class types.

nbcltypes table

Column Name	Type	Null	Key	Default	Description
type	tinyint(4)		PRI	0	
description	char(25)	YES		0	

nbschedules

The nbschedules table contains a list of NetBackup schedule...

nbschedules table

Column Name	Type	Null	Key	Default	Description
classid	smallint(6)		PRI	0	
scheduleid	smallint(6)		PRI	0	
schedulename	varchar(128)				
type	tinyint(4)	YES			
frequency	int(11)	YES			
retentioncode	tinyint(4)	YES			
poolid	smallint(6)	YES			
residence	varchar(40)	YES			

nbwindows

The nbwindows table contains the NetBackup scheduling information for each NetBackup class definition.

nbwindows table

Column Name	Type	Null	Key	Default	Description
classid	smallint(6)		PRI	0	Class identifier. Relates to classid in nbclasses.
scheduleid	smallint(6)		PRI	0	Schedule identifier. Relates to scheduleid in nbschedules.
windowid	tinyint(4)		PRI	0	day of week window pertains to. Sunday = 0
start	int(11)	YES			time of day window opens in seconds from midnight.
duration	int(11)	YES			length of window in seconds.
opentime	int(11)	YES			time window opens in number of seconds since Sunday 00:00
closetime	int(11)	YES			time window closes in number of seconds since Sunday 00:00

nbtypes

The nbtypes table is a lookup table that contains one row for each backup type provided by NetBackup;

nbtypes table

Column Name	Type	Null	Key	Default	Description
type	tinyint(4)		PRI	0	
description	char(25)	YES			

nbmedia

The nbmedia table contains media information from “bpmedialist –l”.

nbmedia table

Column Name	Type	Null	Key	Default	Description
media_id	char(6)		PRI		The media identifier.
partner_id	char(6)	YES			The partner identifier.
version	smallint(6)	YES			The media version.
density_code	smallint(6)	YES			The recording density.
allocated	datetime	YES			The date this piece of media was allocated for use.
last_written	datetime	YES			The most recent date the piece of media was written to.
expiration	datetime	YES			The date the last image will expire.
last_read	datetime	YES			The last time the piece of media was read from.
kbytes	int(11)	YES			The total amount of data stored on the media in Kbytes.
nimages	smallint(6)	YES			total number of images stored on media
vimages	smallint(6)	YES			The total number of virtual images stored on this media.
retention_level	smallint(6)	YES			The retention level assigned to the media.
pool	tinyint(4)	YES			The pool the media belongs to.

nbmedia table

num_restores	smallint(6)	YES			The number of restores performed against this media.
status	smallint(6)	YES			The media status.
ismpx	tinyint(4)	YES			Is this media multiplexed?
isfull	tinyint(4)	YES			Is this media full?
frozen	tinyint(4)	YES			Is this media frozen?
imported	tinyint(4)	YES			Is this media imported?
suspended	tinyint(4)	YES			Is this media suspended?
hsize	smallint(6)	YES			
ssize	smallint(6)	YES			
l_offset	smallint(6)	YES			
psize	smallint(6)	YES			
reserved_off1	smallint(6)	YES			Reserved.
reserved_off2	smallint(6)	YES			Reserved.
res1	smallint(6)	YES			Reserved
res2	smallint(6)	YES			Reserved
res3	smallint(6)	YES			Reserved
res4	smallint(6)	YES			Reserved

nbretention

The nbretention table provides a description of NetBackup retention levels.

Column Name	Type	Null	Key	Default	Description
level	tinyint(4)		PRI	0	The retention level.

duration	int(11)			0	The retention time in seconds.
description	char(40)	YES			A textual description of retention time.

nbstu

The nbstu table contains storage unit data from “bpstulist –l”.

nbstu table

Column Name	Type	Null	Key	Default	Description
label	varchar(128)		PRI		The name of storage unit.
type	tinyint(4)	YES			The type of storage unit.
host	varchar(255)		MUL		The host to which the storage unit is attached.
drives	tinyint(4)	YES			The number of drives in storage unit.
demand	tinyint(4)	YES			
density	tinyint(4)	YES			The recording density.
robot_type	tinyint(4)	YES			The robot type.
robot_number	tinyint(4)	YES			The robot number.
maxfragsize	smallint(6)	YES			The maximum permitted fragment size.
maxmpx	smallint(6)	YES			The maximum multiplex factor.
path	varchar(255)	YES			The device path (disk storage units only).
res1	tinyint(4)	YES			

nbvolumes

The nbvolumes table contains media information from “vmquery –a” and on Windows from “vmquery –a –o”.

nbvolumes table

Column Name	Type	Null	Key	Default	Description
media_id	char(6)		PRI		The media identifier.
media_type	char(20)				The type of media.
optical_partner	char(6)	YES			The name of the optical partner.
bar_code	char(16)	YES			The value of the bar code.
robot_type	char(5)	YES			The type of robot media is resident in.
robot_number	smallint(6)	YES			The number of the robot media is resident in.
slot_number	smallint(6)	YES			The slot media is in.
res2	smallint(6)	YES			Reserved
res3	smallint(6)	YES			Reserved
res4	smallint(6)	YES			Reserved.
res5	smallint(6)	YES			Reserved.
robot_host	varchar(255)	YES			The name of the host to which the robot is attached.
volume_group	char(10)	YES			The volume group to which the media belongs.
num_mounts	smallint(6)	YES			The number of times the media has been mounted.
max_mounts	smallint(6)	YES			The maximum number of permitted mounts.

nbvolumes table

version	smallint(6)	YES			
vm_status	smallint(6)	YES			
last_mounted	datetime	YES			The date the media was last mounted.
first_mounted	datetime	YES			The date the media was first mounted.
created	datetime	YES			The date the media was created.
assigned	datetime	YES			The date the media was assigned.
expiration	datetime	YES			The date the media expires.
poolname	char(20)				The name of pool the media belongs to.
description	char(30)	YES			A textual description of the media.
hostname	varchar(255)		PRI		The name of the host the media is assigned to.

vmpools

The vmpools table contains volume pool information from “vmpools –listall”.

vmpools table

Column Name	Type	Nulls	Key	Default	Description
poolid	smallint(6)		PRI	auto inc.	An artificially created unique key.
retired	date	YES			The date the pool data was retired and archived.
pool	smallint(6)			0	The VERITAS-assigned pool ID.

vmpools table

name	char(20)		MUL		The name of the pool.
description	char(30)	YES			A description of the pool.
host	varchar(255)	YES			The name of the host the pool is assigned to. NULL indicates ANY.
user	char(12)	YES			
ugroup	char(12)	YES			

nbcatalog

The nbcatalog table contains one row for each day with file counts and sizes from the first arloader execution on that day. The catalog backup columns may be updated by subsequent arloader runs.

nbcatalog table

Column Name	Type	Null	Key	Default	Description
catdate	date		PRI	0000-00-00	The date of the snapshot.
fullcompmb	int(11)	YES			Full compressed in MB.
fullcompcnt	int(11)	YES			Full compressed number of files.
fulluncompmb	int(11)	YES			Full uncompressed in MB.
fulluncompcnt	int(11)	YES			Full uncompressed number of files.
incrcompmb	int(11)	YES			Incremental compressed in MB.
incrcompcnt	int(11)	YES			Incremental compressed number of files.
incruncompmb	int(11)	YES			Incremental uncompressed in MB.

nbcatalog table

incruncompcnt	int(11)	YES			Incremental uncompressed number of files.
ubakcompmb	int(11)	YES			User directed compressed in MB.
ubakcompcnt	int(11)	YES			User directed compressed number of files.
ubakuncompmb	int(11)	YES			User directed uncompressed in MB.
ubakuncompcnt	int(11)	YES			User directed uncompressed number of files.
othermb	int(11)	YES			Amount of overhead in MB.
backup_time	datetime	YES			The date and time of the latest catalog backup.
backup_media	char(6)	YES			The ID of the media containing latest catalog backup.

vmstat

The vmstat table contains system performance information obtained on Unix from the vmstat command.

vmstat table

Column Name	Type	Null	Key	Default	Description
stamp	timestamp(14)	YES	PRI		The time of the snapshot.
running	smallint(6)	YES			The number of running processes.
blocked	smallint(6)	YES			The number of blocked processes.

vmstat table

waiting	smallint(6)	YES			The number of waiting processes.
swap	int(11)	YES			The available swap space.
freemem	smallint(6)	YES			The available free memory.
pagein	smallint(6)	YES			The page in per second.
pageout	smallint(6)	YES			The page out per second.
disk1	smallint(6)	YES			The I/O per second.
disk2	smallint(6)	YES			The I/O per second.
disk3	smallint(6)	YES			The I/O per second.
disk4	smallint(6)	YES			I/O per second
usertime	tinyint(4)	YES			% CPU user
systemtime	tinyint(4)	YES			% CPU system
idletime	tinyint(4)	YES			% CPU idle

nblicense

The nblicense table contains license information obtained from NBU's "bpminlicense" command. Each row represents a given feature's license. The validity of a feature's license is stored in license_chk. Only feature licenses associated with NBAR will be stored in this table. If a feature has a license_type in the "permanent" category, the expiration dates will be zero-filled. This table will not keep history. If a feature has a license which supersedes another license for that same feature, only the most inclusive license for that feature will be stored in this table.

nblicense table

Column Name	Type	Null	Key	Default	Description
product_id	int	NO			VERITAS product ID. For example, 6 represents NBU DataCenter

nblicense table

license_chk	Boolean	NO			1=valid license -1= invalid license
feature_id	int	NO	PRI		Will contain one of the following: 31 (NBAR); 28 (GDM server); 50 (GDM Managed Server); 21 (Unrestricted)
product_name	varchar(128)	NO			Such as “NetBackup DataCenter”
product_vers	char(128)	NO			Product release (such as 4.5)
license_date	date	NO			The date this feature’s license was added. (Used when calculating temporary license expiration dates.)
update_date	date	NO			A timestamp of when this row was last changed.
expiration_date	date	NO			A temporary license’s expiration date, as calculated from the date the license was initially added.
firm_expiration	date	NO			A temporary license’s hard-coded end-date. This date is not calculated but is hard coded into the feature’s license key.
license_type	int	NO			SIG Component Group scheme for organizing licenses: 0=Demo; 1,2,3=Permanent; 4=NotForResale; 5=DemoExtension

nbjobfs

The nbjobfs table contains one row for each NBU stream.

nbjobfs table

Column Name	Type	Null	Key	Default	Description
jobid	int		PRI		NBU job ID of the stream.
filesystem	varchar(255)		PRI		The file system or directory handled by the stream.

nbcontrol

The nbcontrol table contains one record for each invocation of the data loader. It is used to avoid duplication of data in nbjobs, nbjobfs and nberrorlog.

nbcontrol table

Column Name	Type	Null	Key	Default	Description
run_init	datetime	YES			The date and time at which loader run started.
run_term	datetime	YES			The date and time at which loader run ended.
run_version	char(12)	YES			The loader version string.
run_type	char(1)	NO			NBAR / GDM
run_server	varchar(255)	YES			For rollup / consolidation.
job_init	datetime	YES			The date and time of first image or error record loaded.
job_term	datetime	Y			The date and time of last image or error record loaded.
job_server	varchar(255)	Y			For rollup / consolidation.
nbu_version	char(12)	Y			The NetBackup version.
hoursago	smallint	Y			From the command line.
pool_count	int	Y			The number of rows in the vmpools table.

nbcontrol table

media_count	int	Y			The number of rows in the nbmedia table.
stu_count	int	Y			The number of rows in the nbstu table.
volume_count	int	Y			The number of rows in the nbvolumes table.
class_count	int	Y			The number of rows in the nbclasses table.
image_count	int	Y			
error_count	int	Y			
job_count	int	Y			The number of inserts to nbjobs during this run.

nbcache

The nbcache table contains data extracted from the NBU error log for jobs which were in progress when the NBAR data loader executed.

nbcache table

Column Name	Type	Null	Key	Default	Description
jobid	int(11)		PRI	auto inc.	An artificially created job identifier. Used to relate NetBackup jobs to entries in the nberrorlog table.
jobtime	datetime		MUL	0000-00-00	The start UTS of the job translated to DB date format.
type	char(1)		MUL		B: backup, R: restore

nbcache table

status	int(11)		MUL	0	-1: error occurred, refer to nberrorlog for NBU error code, 0: Successful job 1: Partially successful job
servername	varchar(255)		MUL		The name of the media server which executed the job.
clientname	varchar(255)		MUL		The name of the client the job was run on.
startuts	int(10)unsigned		MUL	0	The start UTS of the job.
duration	int(10)unsigned			0	The time, in seconds, the job took to complete.
classid	smallint(6)	Y	MUL	0	The class identifier of the NetBackup Class the job ran in. Refers to classid column in nbclasses table. –1 or NULL if unknown.
scheduleid	smallint(6)	Y	MUL	0	The schedule identifier of the NetBackup Class-Schedule the job ran in. Refers to scheduleid column in nbschedules table. –1 or NULL if unknown.
windowid	tinyint(4)	Y		0	The window the job ran in. Digit from 0-6. 0 is Sunday. 10 or NULL if unknown.
windowdate	date	Y	MUL	0000-00-00	Deprecated.
volume	int(10)unsigned			0	The amount of data, in Kbytes, the job processed.

nbcache table

throughput	smallint(6)			0	The average throughput, in Kbytes / second, the job achieved.
nfiles	mediumint(9)			0	The number of files the job processed.
driveindex	tinyint(3)unsigned	YES			The index of the drive used for the job.
poolid	smallint(6)	Y	MUL	0	The pool identifier of the Volume Pool the media was selected from. Relates to poolid in the vmpools table. –1 or NULL if unknown
streamid	int		MUL		The primary job ID for a multistream job.
filesystem	varchar(255)	Y			The file system name.
num_retries	int	N			The tally of “adding job to queue” messages.
backup_id	varchar(255)	Y			A unique ID / link to image

nbarlog

The nbarlog table contains loader error and diagnostic messages

nbarlog table

Column Name	Type	Null	Key	Default	Description
logtime	datetime	N			The timestamp of the message.
severity	tinyint	Y			1:trace 2:engineering 4:warning 8:error 12:severe 16:fatal
program	char(10)	Y			

nbarlog table

helplink	int	Y			The key to documentation of the cause of the error and remedial or diagnostic action.
message_text	varchar(255)	Y			The text of the message.

nbconfig

The nbconfig table contains a log of configuration parameters from nbar.cnf. Keyword-value pairs in nbar.cnf are compared to rows in nbconfig each time arloader executes. A new keyword causes addition of a row to nbconfig. A modified value for an existing keyword causes the row containing the old value to have its term_time set, and a new row to be created containing the new value.

nbconfig table

Column Name	Type	Null	Key	Default	Description
init_time	datetime	N	2		The timestamp at which keyword-value pair was first found.
term_time	datetime	N			The timestamp at which keyword-value pair was last found.
keyword_text	varchar(255)	N	1		The text of the keyword.
value_text	varchar(255)	Y			The value text.

nblookup

The nblookup table is a general-purpose lookup table. Each “table” is identified by a unique table_name, and each row within that table by a unique lookup_code. The string in lookup_text will generally be an expansion of the code. For example, in table_name “robot_type” the lookup_code “TLD” might have a lookup_text value “DLT Library”. In a

hypothetical “airport” table, lookup_code “BOS” would have lookup_text “Logan International Airport, Boston, Massachusetts”. This table may eventually be used for localization.

nblookup table

Column Name	Type	Null	Key	Default	Description
table_name	char(12)	N	1		The name of the (sub) table.
lookup_code	char(12)	N	2		The unique key value for the row.
lookup_text	varchar(255)	N			The text of the keyword.

nbdrive

The nbdrive table contains one row for each backup device attached to a master or media server, refreshed by arloader during each execution from the output of “vmoprcmd –xdraw”.

nbdrive table

Column Name	Type	Null	Key	Default	Description
media_server	varchar(255)	N			The fully-qualified name of a media server.
version	char(20)	Y			For example, DRIVESTATUS3.2
drive_index	tinyint	N			For example, 0, 1, 2, …
type	char(5)	Y			For example, hcart, dlt, …
control	char(8)	Y			For example, DOWN, DOWN_LMF, AVR, …
user	char(8)	Y			For example, NULL, root, …
rvsn	char(6)	Y			
evsn	char(6)	Y			

nbdrive table

request_id	char(8)	Y			
robot_type	char(5)	Y			
robot_number	tinyint	Y			
flags	char(8)	Y			
drive_name	char(20)	Y			
assigned_host	varchar(255)	Y			
scan_host	varchar(255)	Y			
last_cleaning	datetime	Y			
comment	varchar(255)	Y			

GDM Table Definitions

Type 1 – GDM Tables on the NBAR Master Servers

These tables reside on each NBU master server in the NBAR GDM domain and contain summary information about the NBU activities happening on that local server. These tables are created and maintained by arpusher.pl.

gdmnbstat

The gdmnbstat table is used to rollup information to be used on the GDM Global Error Details report. For every unique status code issued on the NBU master, there will exist a row showing how many jobs completed with that status code for the given report day.

gdmnbstat table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data.
statusCode	tinyint	No	PRI	0	The NetBackup status code.
JobCount	Int	No		0	The number of jobs having this NBU status code.
pushFlag	Tinyint	No	MUL	0	The flag to tell the arpusher program whether this row should be inserted (1) on GDM server or updated (2) on GDM server.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

gdmsitsiz

The gdmsitsiz table is used to rollup information to be used on the GDM Global Site Size report. A row exists for each day showing the size of the NBU catalog.

gdmsitsiz table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data.
catalogSize	int	No		0	The NBU catalog size in Kbytes.
dbFileCount	int	No		0	The number of .f files in the NBU catalog.
classCount	smallint	No		0	The total number of classes.
clientCount	int	No		0	The total number of clients.
pushFlag	Tinyint	No	MUL	0	A flag to tell the arpusher program whether this row should be inserted (1) on the GDM server or updated (2) on the GDM server.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

gdmbkgrow

The gdmbkgrow table is used to rollup information to be used on the GDM Global Backup Growth report. For every media server running on this master server, there will exist a row showing how much volume has been backed up for a given day.

gdmbkgrow table

Column Name	Type	Null	Key	Default	Description

gdmbkgrow table

reportDay	date	No	PRI		The day associated with this NBU data.
mediaServer	varchar(255)	No	PRI		The media server associated with this backup data.
volume	int	No		0	The amount of data backed up in Kbytes.
fileCount	int	No		0	The number of files backed up.
stunitCount	smallint	No		0	The number of storage units defined to this media server.
driveCount	smallint	No		0	The number of drives defined to this media server.
pushFlag	Tinyint	No	MUL	0	A flag to tell the arpusher program whether this row should be inserted (1) on GDM server or updated (2) on GDM server.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

gdmmeduse

The gdmmeduse table is used to rollup information to be used on the GDM Global Media Usage report. For every unique robot number / media type combination on this master server, there will exist a row containing information about its media inventory for the given day.

gdmmeduse table

Column Name	Type	Null	Key	Default	Description

gdmmeduse table

reportDay	date	No	PRI		The day associated with this NBU data.
deviceKey	smallint	No	PRI		An artificial key to order media into robot / media categories.
robotNumber	int				
robotType	string	No			The NBU code that identifies the robot type.
mediaType	string				The NBU code that identifies the media type.
total	int	No		0	The total number of media.
available	int	No		0	The number of available media.
active	int	No		0	The number of media assigned to NBU.
fullCount	int	No		0	The number of full media assigned to NBU.
frozen	int	No		0	The number of frozen NBU media.
suspended	int	No		0	The number of suspended NBU media.
recycle	int	No		0	The number of full NBU media qualifying for being recycled as of a given date.
fullVolumeAvg	int	No		0	An average volume (in Kbytes) of all full NB media.

gdmmeduse table

pushFlag	Tinyint	No	MUL	0	A flag to tell the arpusher program whether this row should be inserted (1) on GDM server or updated (2) on GDM server.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

gdmstatus

The gdmstatus table holds status information to be used on the Daily GDM Rollup report. A row is created each time the server successfully rolls up its NBU data and pushes that data to the GDM server.

gdmstatus table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data.
startProc	datetime	No	PRI		The time this iteration of rollup processing began (local server time).
endProc	datetime	No			The time this iteration of rollup processing completed (local server time).
jobsInProgress	smallint	No		0	The number of jobs in nbcache during this iteration of rollup processing.
gmtOffset	Int	No		0	+/- minutes difference between a managed server's time and the GDM server's time.

gdmstatus table

pushFlag	Tinyint	No	MUL	0	A flag to tell the arpusher program whether this row should be inserted (1) or updated (2) on GDM server.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

gdmsysinf

The gdmsysinf table holds product version information to be used in the GDM System Information report. This report is deferred for NBAR 4.5 but the data is being captured now.

gdmsysinf table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data
nbarVersion	string	No	PRI		The NBAR version information.
nbuVersion	string	No			The NBU version information.
nbuDcBs	tinyint	No		0	A Boolean describing this installation of NBU as DataCenter or BusinesServer.
pushFlag	tinyint	No		0	A flag to tell the arpusher program whether this row should be inserted (1) or updated (2) on the GDM server.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

GDM Table Definitions

Type 2 – GDM Tables on the GDM server.

These tables reside on the GDM server only. They contain all of the data in the type 1 GDM tables from all of the NBAR servers in the NBAR GDM domain. These tables are created and maintained by arpusher.

nbserver

The nbserver table is a special case. It is updated by the customer using a configuration utility. It contains information needed by about the servers being managed in the GDM domain. This table resides on the GDM server only.

nbserver table

Column Name	Type	Null	Key	Default	Description
masterserver	varchar(255)	No	PRI		The name of the managed server being controlled by the GDM server.
rollupSched	time	No			The approximate time this managed server will start the arpusher program each day.
dormantThresh	smallint	No		0	The number of days to be added to the media expiration date before a piece of media is considered a candidate for recycling.
sord	time	No			An acronym for the Start-Of-Reporting-Day. A local cutoff time for this server that determines what reportDay to place NBU activity.

nbserver table

lastUpdate	timestamp				The timestamp of the latest activity on this row.

momnbstat

The momnbstat table is used to summarize information onto the master of masters (GDM server) to be used to create the GDM Global Error Details report. For every unique status code issued on each NBU master server, there will exist a row showing how many jobs completed with that status code on that day on that server.

momnbstat table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data.
masterServer	varchar(255)	No	PRI		
statusCode	tinyint	No	PRI	0	The NBU status code.
JobCount	Int	No		0	The number of jobs having this NBU status code.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

momsitsiz

The momsitsiz table is used to summarize information onto the GDM server to be used to create the GDM Global Site Size report. A row exists for each master server for each day showing the size of the NBU catalog.

momsitsiz table

Column Name	Type	Null	Key	Default	Description

momsitsiz table

reportDay	date	No	PRI		The day associated with this NBU data.
masterserver	varchar(255)	No	PRI		
catalogSize	int	No		0	The NBU catalog size in Kbytes.
dbFileCount	int	No		0	The number of .f files in the NBU catalog.
classCount	smallint	No		0	The total number of classes.
clientCount	int	No		0	The total number of clients.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

mombkgrow

The mombkgrow table is used to summarize information onto the GDM server to be used to create the GDM Global Backup Growth report. For every media server running on every master server in the GDM domain, there will exist a row showing how much volume has been backed up on a given day.

mombkgrow table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data.
masterserver	varchar(255)	No	PRI		
mediaServer	varchar(255)	No	PRI		The media server associated with this backup data.
volume	int	No		0	The amount of data backed up in Kbytes.

mombkgrow table

fileCount	int	No	0	The number of files backed up.
stunitCount	smallint	No	0	The number of storage units defined to this media server.
driveCount	smallint	No	0	The number of drives defined to this media server.
lastUpdate	timestamp			Timestamp of latest activity on this row.

mommeduse

The mommeduse table is used to summarize information onto the GDM server to be used to create the GDM Global Media Usage report. For each day, for every unique robot number / media type combination associated with every master server in the GDM domain, there will exist a row containing information about the media inventory.

mommeduse table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data.
masterserver	varchar(255)	No	PRI		
deviceKey	smallint	No	PRI		An artificial key to order media into robot / media categories.
robotNumber	int				
robotType	string	No			An NBU code identifying robot type.
mediaType	string	no			An NBU code identifying media type.
total	int	No		0	The total number of media.

mommeduse table

available	int	No	0	The number of available media.
active	int	No	0	The number of m.edia assigned to NBU
fullCount	int	No	0	The number of full media assigned to NBU.
frozen	int	No	0	The number of frozen NBU media
suspended	int	No	0	The number of suspended NBU media.
recycle	int	No	0	The number of full NBU media qualifying for being recycled as of a given date.
fullVolumeAvg	int	No	0	An average volume (in Kbytes) of all full NB media.
lastUpdate	timestamp			The timestamp of the latest activity on this row.

momstatus

The momstatus table is used to summarize information onto the GDM server to be used to create the Daily GDM Rollup report. A row exists for each time a master server successfully connects and pushes its NBAR data to the GDM server.

momstatus table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data.
masterserver	varchar(255)	No	PRI		

momstatus table

startProc	datetime	No	PRI		The date this iteration of rollup processing began (local server time).
endProc	datetime	No			The date this iteration of rollup processing completed (local server time).
jobsInProgress	smallint	No		0	The number of jobs in nbcache during this iteration of rollup processing.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

momsysinf

The momsysinf table holds product version information to be used in the GDM System Information report. This report is deferred for NBAR 4.5 but the data is being captured now.

momsysinf table

Column Name	Type	Null	Key	Default	Description
reportDay	date	No	PRI		The day associated with this NBU data.
masterserver	varchar(255)	No	PRI		
nbarVersion	string	No			The NBAR version information.
nbuVersion	string	No			The NBU version information.
nbuDcBs	tinyint	No		0	A Boolean describing NBU as DataCenter or BusinesServer.

momsysinf table

pushFlag	tinyint	No		0	A flag to tell the arpusher program whether this row should be inserted (1) or updated (2) on GDM server.
lastUpdate	timestamp				The timestamp of the latest activity on this row.

Glossary

access control list (ACL)

Security information associated with files on some file systems.

ACS

Automated Cartridge System. This robot type is supported only by NetBackup DataCenter servers.

active job

A job for which NetBackup is currently processing backup or restore data.

activity logs

See “debug logs.”

activity monitor

A NetBackup administration utility that displays information about NetBackup jobs and provides limited control over them.

administration client

See “remote administration console.”

administrator

A user that is granted special privileges to install, configure, and manage the operation of a system, network, or application

AIT

Sony Advanced Intelligent Tape, a type of tape drive or media type.

alternate-client restore

See “redirected restore (different client).”

alternate-target restore

See “redirected restore (different target).”

alternate path restore

See “redirected restore (different path).”

archive

A special kind of backup where NetBackup backs up the selected files, and if the backup is successful, deletes the files from the local disk. In this manual, references to backups also apply to the backup portion of archive operations except where otherwise noted.

archive bit

A file-status bit that the Microsoft based operating system sets when it writes a file, thereby indicating that the file has changed.

attributes for a policy

Configuration parameters that control the behavior of NetBackup during operations involving this policy.

autochanger

See “robotic library.”

autoloader

See “robotic library.”

automatic backup

A scheduled backup by the master server.

back up

The act of copying and saving files and folders to storage media.

backup

Refers to the process of copying and saving files and directories to storage media. For example, *the backup is complete*. This term can also refer to the collection of data that NetBackup saves for a client during a backup or archive. For example, *duplicate the backup*.

Backup is two words when used as a verb. For example, *back up the file*.

backup, archive, and restore interface

The name of the NetBackup Microsoft Windows and Java based user interfaces for clients. On servers, these interfaces can be started through the NetBackup Administration Console.

backup window

The period of time during which backups can begin.

block size

The number of bytes in each block of data written on the media during a backup.

bp

A backup, archive, and restore utility for users on NetBackup UNIX clients. It has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

bpadm

An administrator utility that runs on NetBackup UNIX servers. It has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

bp.conf file

A NetBackup configuration file on UNIX servers and also on UNIX, Macintosh, and OS/2 clients.

bp.ini file

NetBackup initialization file for Novell NetWare target clients.

bpcd

NetBackup Client service on Windows and the NetBackup Client daemon on UNIX.

bprd

NetBackup Request Manager service on Windows and NetBackup Request daemon on UNIX.

cancel a job

Terminating a job and removing it from the job queue.

carousel

See “robotic library.”

catalogs

Internal NetBackup and Media Manager databases. These catalogs contain information about configuration, media, devices, status, errors, and the files and directories in the stored backup images.

CDF

Context-dependent file, which is a type of directory structure on a Hewlett-Packard system.

changer

See “robotic library.”

class

See “policy.”

client

The system with the files to back up, archive, or restore.

client-user interface

See “user interface.”

cluster

See master and media server cluster.

command lines

Commands that users can execute either from the system prompt or in scripts.

compression

The process of compacting data to enable more efficient transmission and storage.

configuration

The parameters that govern the behavior of an application. This term can also refer to the manner in which a network or system is laid out or connected (for example, a network configuration).

cpio

A UNIX command that can be used for copying files to or from a cpio archive on disk or tape.

ctime

The time that a UNIX inode was changed.

cumulative-incremental backup

A backup that is scheduled by the administrator on the master server and backs up files that have changed since the last successful full backup. All files are backed up if no prior backup has been done. Also see “differential-incremental backup.”

daemon

A program on a UNIX system that runs in the background and performs some task (for example, starting other programs when they are needed). Daemons are generally referred to as services or processes on Windows server systems.

database-agent clients

Clients with additional NetBackup software that is designed to back up relational databases.

database-extension clients

See “database-agent clients.”

debug logs

Logs that can be optionally enabled for specific NetBackup and Media Manager programs and processes and then used to investigate problems.

device delays

Delays caused by the device that are beyond the control of the storage application. An example is the time required to position tape under the read and write heads.

device host

A host (that has Media Manager installed) where a drive or robotic control is attached or is defined.

device monitor

A Media Manager administration utility that provides monitoring and manual control of Media Manager storage devices. For example, an administrator or computer room operator can use this utility to manually reset devices or set them to the UP or DOWN state.

DHCP

Dynamic host configuration protocol. This TCP/IP protocol automatically assigns temporary IP addresses to hosts when they connect to the network.

differential-incremental backup

Scheduled by the administrator on the master server and backs up files that have changed since the last successful incremental or full backup. All files are backed up if no prior backup has been done. Also see “cumulative-incremental backup.”

directory depth

The number of levels below the current directory level that the NetBackup interfaces show in their directory and file list displays.

directory tree

The hierarchical structure in which files are organized on a disk. Each directory lists the files and directories that are directly below it in the tree. On UNIX, the topmost directory is called the root directory.

disaster recovery

Recovering data from backups after a disk crash or other catastrophe.

disk

Magnetic or optical disk storage media.

disk-image backup

A bit-by-bit rather than a file system backup of a disk drive on a Windows platform.

DLT

Digital-linear tape or tape drive type.

Domain Name Service (DNS)

A program that handles name translation for network communications.

drive cleaning

The use of a special cleaning tape to clean the heads on a drive.

duplicate image

A copy of a backup image.

eject

Move media out of a robotic library.

encryption

Provides additional security by encrypting backup data on the client. This capability is available only with the NetBackup Encryption option.

entry and exit ports

See “media access port.”

exclude list

A list that designates files or directories to exclude from automatic backups.

expiration (image)

The date and time when NetBackup stops tracking a backup image.

expiration (volume)

The date and time when the physical media (tape) is considered to be no longer usable.

external media ID

This is an identifier written on a media cartridge or canister to help the operator identify the volume before inserting it into a drive or robot. For labeled media, the external media ID should be the same as the media ID recorded on the media.

EVSN

See “external media ID.”

FlashBackup

A special type of raw-partition backup that requires the NetBackup FlashBackup separately-priced option (this option is available only for NetBackup DataCenter).

flush level

Controls how often Netbackup clears its log files on a Novell NetWare or Microsoft Windows client platform.

fragment

A part of a backup or archive image. NetBackup can be configured to divide images into fragments when they exceed a certain size or span tapes.

frequency (backup)

How often NetBackup performs scheduled backups. For example, if the frequency is seven days then backups occur once a week.

FROZEN media state

If a volume is FROZEN, NetBackup keeps it indefinitely and can restore from it but not use it for further backups or archives.

full backup

A backup that copies, to a storage unit, all files and directories that are beneath a specified directory.

FULL media state

If this appears in a report or listing, it indicates the volume is FULL and cannot hold more data or be used for further backups.

global attributes

NetBackup configuration attributes that affect all policies.

GDM Dashboard

The name for the Global Data Manager interface. The Dashboard enables monitoring job and drive activity on multiple master servers, as well as providing alerts to problem conditions.

GDM Managed Server

A NetBackup master server that appears as a managed master server in the left pane of the GDM Dashboard.

GDM Server

A NetBackup master server that has the Global Data Manager license activated. When logging into this host, the user can monitor the activity on multiple master servers using the GDM Dashboard interface. If the host has installed the Advanced Reporter option, the reports show information on multiple master servers.

Global Data Manager (GDM)

A separately-priced option (for UNIX servers) that provides an interface with a tree view where the administrator can view and administer multiple master servers. The server where the option is installed is called a GDM Server.

GNU tar

A public domain version of the UNIX tar program.

goodies directory

A directory containing programs, scripts, and other files that are not formally supported.

GUI

Graphical user interface.

hard link

On UNIX, a hard link is a pointer to the inode for the data. On a Windows server, a hard link is a directory entry for a file. Every file can be considered to have at least one hard link. On NTFS volumes each file can have multiple hard links, and a single file can appear in many directories (or even in the same directory with different names).

heap level

A parameter for memory-heap debugging on a Novell NetWare or Windows NetBackup client.

hierarchical storage management

The process of automatically migrating selected files from a managed file system to specified migration levels on secondary storage, while maintaining transparent access to those files.

host

A computer that executes application programs.

host name

Name by which a host computer is identified by programs and other computers in the network.

HSM

See storage migrator.

image

The collection of data that NetBackup saves for an individual client during each backup or archive. The image contains all the files, directories, and catalog information associated with the backup or archive.

import

The process of recreating NetBackup records of images so the images can be restored.

include list

A list that designates files or directories to add back in from the exclude list.

incremental backup

See “cumulative-incremental backup” and “differential-incremental backup.”

inject

Move media into a robotic library.

inport

See “media access port.”

inode

A UNIX data structure that defines the existence of a single file.

install_path

Directory where NetBackup and Media Manager software is installed. The default on Windows servers is `C:\Program Files\VERITAS` and on UNIX it is `/usr/openv`.

jbpSA

The Java-based NetBackup interface for performing user backups, archives, and restores.

jnbSA

The Java-based NetBackup interface for administrators.

job

A parcel of work submitted to a computer. NetBackup jobs are backups, archives, or restores.

kernel

The nucleus of an operating system.

keyword phrase

A textual description of a backup.

kill a job

See “cancel a job.”

label

Identifier of a tape or optical disk volume. A recorded label includes a media ID.

A barcode label allows a barcode scanner to be used for media tracking.

library

See “robotic library.”

link

See “hard link” or “symbolic link.”

LMF - Library Management Facility

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

This robot type is supported only by NetBackup DataCenter servers.

load

(noun) Amount of work that is being performed by a system or the level of traffic on a network. For example, network load affects performance.

(verb) Copy data to internal memory. For example, load the installation program.

(verb) Used to indicate tape drive initialization done when new media is being added.

logs

Files where a computer or application records information about its activities.

mailslot

See “media access port.”

man pages

Online documentation provided with UNIX computer systems and applications.

Master and media server cluster

A NetBackup master server and the remote media servers that it is using for additional storage. It is possible to configure clusters only with NetBackup DataCenter servers. NetBackup BusinesServer supports only a single server, the master.

Master of Masters

A NetBackup host where Global Data Manager software is installed. When logging into this host, the interface has a tree view where the administrator can view and administer multiple master servers.

master server

The NetBackup server that provides administration and control for backups and restores for all clients and servers in a master and media server cluster. NetBackup BusinesServer supports only a single server and it is the master.

media

Physical magnetic tapes, optical disks, or magnetic disks where data are stored.

media access port

A slot or other opening in a robot where you can insert or remove a tape without having to access the interior of the robot. After inserting a tape, you move it to a slot by using an inject command. Prior to removing a tape, you move it to the port by using an eject command. The inject and eject commands are supported through the add and move screens in the Media Manager administration interface.

media host

NetBackup server to which the job (client) is sending the data.

media ID

An identifier that is written on a volume as part of the recorded label.

Media Manager

Software that is part of NetBackup and manages the storage devices and removable media.

Media Manager Host

Host where Media Manager is installed (may have devices attached)

media server

A NetBackup server that provides storage within a master and media server cluster. The master can also be a media server. A media server that is not the master is called a remote media server. NetBackup BusinesServer does not support remote media servers.

menu interface

A character-based interface for use on terminals that do not have graphical capabilities.

mount

Make a volume available for reading or writing.

mount point

The point where a file system on a disk logically connects to a system's directory structure so the file system is available to users and applications.

MPX

See "multiplexing."

mtime

The point in time when a UNIX or NTFS file is modified.

multiplexing

The process of sending concurrent-multiple backups from one or more clients to a single storage device and interleaving those images onto the media.

multiplexed group

A set of backups that were multiplexed together in a single multiplexing session.

NDMP

Network data management protocol. NetBackup requires the NetBackup for NDMP separately-priced option to support NDMP.

NetBackup Client service

NetBackup Windows service that runs on clients and servers and listens for connections from NetBackup servers and clients in the network. When a connection is made, this service starts the necessary programs.

NetBackup configuration options

On UNIX servers and on UNIX and Macintosh, clients, these settings are made in the `bp.conf` file. On NetWare target and OS/2 clients, they are in the `bp.ini` file. On Windows servers and Windows clients, these settings are called properties and are made through the Backup, Archive, and Restore interface or the Host Properties dialog in the NetBackup Administration Console.

NetBackup databases

See catalogs.

NetBackup Database Manager service

NetBackup Windows service that runs on the master server and manages the NetBackup internal databases (called catalogs). This service must be running on the master server during all NetBackup administrative operations.

NetBackup Device Manager service

The NetBackup Windows service that runs on a NetBackup server and starts the robotic control processes and controls the reservation and assignment of volumes. This service runs only if the server has devices under Media Manager control. The process is `ltid`.

NetBackup properties

Same as NetBackup configuration options but are called NetBackup properties on Microsoft Windows platforms.

NetBackup Request Manager service

The NetBackup Windows service that runs on the master server and starts the scheduler and receives requests from clients.

NetBackup Volume Manager service

A NetBackup Windows service that runs on a NetBackup server, allows remote administration of Media Manager, and manages volume information. The process is `vmd`.

NIS

Network information service.

NLM

NetWare loadable module.

NFS

Network file system.

nonrobotic

See “standalone.”

ODL

Optical disk library. This robot type is supported only by NetBackup DataCenter servers.

outport

See “media access port.”

partitions

The logical partitions into which a magnetic disk is divided.

patch

A program that corrects a problem or adds a feature to an existing release of software.

path length

Number of characters in a pathname.

pathname

The list of directories in the path to a destination directory or file.

PC clients

NetBackup clients that have Microsoft Windows, Macintosh, or IBM OS/2 operating systems.

peername

The name by which a computer identifies itself when establishing connections to other systems.

policy

Defines the backup characteristics for a group of one or more clients that have similar backup requirements.

port

A location used for transferring data in or out of a computer.

Also see “media access port.”

primary copy

The copy of an image that NetBackup uses to satisfy restores. When NetBackup duplicates an image, the original is designated as the primary copy.

privileges

The tasks or functions that a user, system, or application is authorized to perform.

profile

A vault profile is a way to save configuration settings. Specific parameters for duplication, catalog backup, eject, and report or any combination of these steps, are configured within a profile.

progress report

Log where NetBackup records events that occur during user operations.

proxy restore

A proxy restore allows the user to restore files that he has write access to, on a machine other than his desktop. The files must be in a backup of the machine to which they are being restored.

QIC

Quarter-inch-cartridge tape.

queued job

A job that has been added to the list of jobs to be performed.

raw-partition backup

Bit-by-bit backup of a partition of a disk drive on UNIX. On Windows, this is called a disk-image backup.

rbak

The program that Apollo clients use to read data from tape during a restore.

recorded media ID

This is an identifier written as part of the label on a volume and used by Media Manager to ensure that the correct volume is mounted. The recorded media ID should match the external media ID.

redirected restore (different client)

Restoring files to your client when they were originally backed up from a different client. The administrator using the interface on the master server can direct a restore to any client (this variation is called a server directed restore).

redirected restore (different target)

On a Novell NetWare server platform running the NetBackup target version of client software, this operation restores files to a different target than the one from which they were backed up.

redirected restore (different path)

Restores files to a different directory than the one from which they were backed up.

registry

A Microsoft Windows database that has configuration information about hardware and user accounts.

remote administration console

A Windows NetBackup client that has the administration interface software installed and can be used to administer NetBackup servers.

remote media server

A media server that is not the master. Note that only NetBackup DataCenter supports remote media servers. NetBackup BusinesServer supports only a single server, the master.

residence

In Media Manager, information about the location of each volume is stored in a volume database. This residence entry contains information, such as robot number, robot host, robot type, and media type.

resource

A Novell NetWare term that refers to a data set on the target. For example, in DOS, resources are drives, directories, and files. Also see “target service.”

restore

(verb) The act of restoring selected files and directories from a previous backup or archive and returning them to their original directory locations (or to a different directory).

(noun) The process of restoring selected files and directories from a previous backup and returning them to their original directory locations (or to a different directory).

retention level

An index number that corresponds to a user-defined retention period. There are 10 levels from which to choose (0 though 9) and the retention period associated with each is configurable. Also see “retention period.”

retention period

The length of time that NetBackup keeps backup and archive images. The retention period is specified on the schedule.

robotic arm

The component of a robotic library that physically selects the media (tape or optical disk).

robotic library

Refers to a robot and its accompanying software. A robotic library includes a collection of tapes or optical platters used for data storage and retrieval. For example, a Tape Library DLT (TLD) refers to a robot that has TLD robotic control.

root

The highest level directory in a hierarchical directory structure. In MS-DOS, the root directory on a drive is designated by a backslash (for example, the root on drive C is C:\). On UNIX, the root directory is designated by a slash (/).

Also, a UNIX user name having administration capability.

RS-232

An industry-standard interface for serial communications and sometimes used for communicating with storage peripherals.

RSM Interface

Application in Windows 2000 used to manage Removable Storage Manager (RSM) devices.

RSM - Removable Storage Manager

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

Also, a component of the Windows 2000 operating system that manages storage devices.

RVSN

See “recorded media ID.”

schedules

Controls when backups can occur in addition to other aspects of the backup, such as: the type of backup (full, incremental) and how long NetBackup retains the image.

SCSI

Small computer system interface. This is a type of parallel interface that is frequently used for communicating with storage peripherals.

server-directed restore

Using the user interface on the master server to restore files to any client. Only the administrator can perform this operation.

server independent restore

Restoring files by using a NetBackup server other than the one that was used to write the backup. This feature is available only with NetBackup DataCenter.

server list

The list of servers that a NetBackup client or server refers to when establishing or verifying connections to NetBackup servers. On a Windows server and Microsoft Windows clients, you update the list through a dialog box in the interface. On a UNIX server and UNIX and Macintosh clients, the list is in the `bp.conf` file. On NetWare target and OS/2 clients, the list is in the `bp.ini` file.

service

A program on a Windows server system that runs in the background and performs some task (for example, starting other programs when they are needed). Services are generally referred to as daemons on UNIX systems.

session

An instance of NetBackup checking its schedules for backups that are due, adding them to its worklist, and attempting to complete all jobs in the worklist. For user backups and archives, a session usually consists of a single backup or archive.

Session (Vault)

A vault session consists of executing a particular profile or profiles.

shared drives

See “Shared Storage Option (SSO).”

Shared Storage Option (SSO)

A separately priced VERITAS software option that allows tape drives (standalone or in a robotic library) to be dynamically shared among multiple NetBackup and Storage Migrator servers.

This option is supported only on NetBackup DataCenter servers.

SMDR

Storage management data requestor, a Novell NetWare program that provides its services transparently to all SMS modules and lets remote and local modules communicate with one another.

SMS

Novell NetWare storage management services.

SSO

See “Shared Storage Option (SSO).”

stacker

Usually a small robotic library that contains one drive only. See “robotic library.”

standalone

A qualifier used with drives and media to indicate they are not associated with a robot. For example, a standalone tape drive is one where you must manually find and insert tapes before using them. A standalone volume is one that is located in a standalone drive or is stored outside of a drive and designated as standalone in the volume configuration.

status code

A numerical code, usually accompanied by a troubleshooting message, that indicates the outcome of an operation.

storage migrator

Refers to the VERITAS Storage Migrator line of hierarchical storage management products for UNIX and Windows. These products make extra room on a disk by transparently moving data to other storage and then transparently retrieving the data when it is needed by a user or application.

Storage Migrator is available only for NetBackup DataCenter servers.

storage unit

Refers to a storage device where NetBackup or Storage Migrator stores files. It can be a set of drives in a robot or consist of one or more single tape drives that connect to the same host.

SUSPENDED media state

If a volume is SUSPENDED, NetBackup can restore from it but cannot use it for backups. NetBackup retains a record of the media ID until the last backup image on the volume expires.

symbolic link

On a UNIX system, this is a pointer to the name of the file that has the source data.

TapeAlert

Allows reactive cleaning for most drive types and is a function of the tape drive.

tape format

The format that an application uses to write data on a tape.

tape marks

A mark that is recorded between backup images on a tape.

tape overhead

The space required for data that is not part of the backup images. For example, tape marks and catalogs of what are on the tape are considered overhead.

tape spanning

Using more than one tape to store a single backup image.

tar

Tape Archive program that NetBackup uses to extract backup images during a restore.

target

See “target service.”

target service

A Novell NetWare service that needs storage management. The SMS views all services (for example, print services, communication services, workstations) as targets.

Target Service Agent

A Target-service agent is a Novell NetWare agent that prepares the target's data for SMS during a backup and for the target during a restore.

TLD - Tape Library DLT

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

TLH - Tape Library Half-inch

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

This robot type is supported only by NetBackup DataCenter servers.

TLM - Tape Library Multimedia

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

This robot type is supported only by NetBackup DataCenter servers.

TL4 - Tape Library 4MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

TL8 - Tape Library 8MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

timeout period

The period of time that an application has allotted for an event to occur.

TIR

See “true image restore.”

tpconfig

A Media Manager administration utility for configuring devices which is started from the command line. On UNIX, it has a character-based menu interface that can be run from terminals that do not have X Windows capabilities. tpconfig also has a command line interface.

transfer rate

The rate at which computer information is transferred between a source and a destination.

transport

See “robotic arm.”

true image restore

Restores the contents of a directory to what it was at the time of any scheduled full or incremental backup. Previously deleted files are ignored.

TS8 - Tape Stacker 8MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

TSA

See “Target Service Agent.”

TSD - Tape Stacker DLT

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

TSH - Tape Stacker Half-inch

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

This robot type is supported only by NetBackup DataCenter servers.

user interface

The program used to perform user backups, archives, and restores.

user operation

A backup, archive, or restore that is started by a person on a client system.

Vault

Vault is a separately-priced NetBackup option that provides offsite backup management. Vault automatically duplicates specified backup images, and automates the process of offsite media rotation (a critical component of any backup or disaster recovery strategy). Vault manages offsite storage and retrieval of media for original backups, duplicate backups, and catalog backups. Additionally, NetBackup Vault generates reports to track the location and content of each piece of media.

vault

In the context of the NetBackup Vault, a vault is logical entity associated with a particular robot that acts as a desginated holding place for backups that will eventually be sent to a physical offsite vault. The term ‘vault’ is used to refer both to the process, and to the physical storage location of a set of tapes offsite.

vault process

Vaulting is the process of choosing backup images to duplicate or eject, optionally duplicating backups, ejecting duplicate or original media, storing it at an offsite location, and later returning expired media to your robot. Vaulting is an integral part of the disaster recovery process.

verbose flag

Configuration file entry that causes a higher level of detail to be written in the logs.

verify

An operation that compares the list of files that are actually on a volume with what NetBackup has recorded as being on it. The data that is on the media is not verified.

vmadm

A Media Manager administrator utility for managing volumes. It runs on UNIX and has a character-based, menu interface that can be run from terminals.

vm.conf

A Media Manager configuration file with entries that include the servers that can manage local devices and default media ID prefixes for media that do not contain barcodes.

volume

Media Manager volumes are logical units of data storage or cleaning capability on media that have been assigned media IDs and other attributes, which are recorded in the Media Manager volume database.

volume configuration

Refers to configuration information that is stored in the Media Manager volume database.

volume database

An internal database where Media Manager keeps information about volumes. All hosts (where Media Manager is installed) have a volume database. However, the database is empty unless the host is designated as a volume database host.

volume database host

The host (where Media Manager is installed) that contains information about the volumes that Media Manager uses in a device. Because NetBackup BusinesServer supports only a single server, the volume database host is always on the same server.

volume group

A set of volumes that are configured within Media Manager to reside at the same physical location (for example, in a specific robot).

volume pool

A set of volumes that are configured within Media Manager to be used by a single application and are protected from access by other applications and users.

wakeup interval

The time interval at which NetBackup checks for backups that are due.

wildcard characters

A character that can be used to represent other characters in searches.

Microsoft Windows

(noun) Describes a line of operating systems developed by Microsoft, Inc.

For more information on the Windows operating systems that NetBackup supports, refer to the VERITAS support web site at `http://www.support.veritas.com`.

Windows

(adjective) Used to describe a specific product or clarify a term. Some examples are: Windows 95, Windows 98, Windows NT, Windows 2000, Windows servers, Windows clients, Windows platforms, Windows hosts, and Windows GUI.

Windows servers

A term that defines the Windows server platforms that NetBackup supports; those platforms are: Windows NT and 2000.

Windows clients

A term that defines the Windows client platforms that NetBackup supports; those platforms are: Windows 95, 98, ME, NT, 2000, XP (for 32- and 64-bit versions), and LE.

Windows Display Console

A NetBackup-Java interface program that runs on Windows 2000, NT, 98, and 95 computers. Users can start this interface on their local system, connect to a UNIX system that has the NetBackup-Java software installed, and then perform any user operations that their permissions allow.

WORM media

Write-once, read-many media for optical disks. NetBackup BusinesServer does not support WORM media.

xbp

The X Windows-based backup, archive, and restore program for users on NetBackup UNIX clients.

Index